広　報　資　料
平成30年３月22日
警　　察　　庁

平成29年中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

(1)　サイバー空間における探索行為等

○　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1,893.0件と引き続き増加。

○　世界的規模で、「WannaCry」等のランサムウェアに悪用された攻撃ツールを用いた攻撃活動等を観測。

○　28年からアクセス件数が引き続き増加している主な要因としては、IoT機器を標的とした攻撃活動等が、年間を通じて高い水準で推移したことが挙げられる。

(2)　サイバー攻撃の情勢及び取組

ア　情勢

○　警察と先端技術を有する事業者等との情報共有の枠組みを通じて報告を受けた標的型メール攻撃は、6,027件と引き続き増加。標的型メール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90％を占めた。

○　国際的ハッカー集団「アノニマス」を名乗る者が、65組織に関して、サイバー攻撃を実行したとする犯行声明とみられる投稿をSNS上に掲載。

イ　取組

○　上記枠組みにおいて、集約された情報等を総合的に分析し、事業者等に対し、分析結果に基づく情報提供を実施。

○　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攻撃インフラ（C2サーバ61台）の機能停止を促進。

○　2020年東京オリンピック・パラリンピック競技大会に向け、関係機関等との共同対処訓練、情報交換等の取組を推進。

２　サイバー犯罪の情勢等

(1)　サイバー犯罪の検挙件数及びサイバー犯罪等に関する相談件数

サイバー犯罪の検挙件数は9,014件と引き続き増加。相談件数は13万11件と引き続き高い水準。

(2)　インターネットバンキングに係る不正送金事犯の発生状況等

○　発生件数は425件と、ピーク時の平成26年と比較して４分の１以下に減少。

○　被害額は約10億8,100万円と、ピーク時の平成27年と比較して約３分の１に減少。

○　金融機関によるモニタリングの強化、ワンタイムパスワードの導入等の対策により、近年被害が大幅に減少。

○　被害金融機関としては、ここ３年で信用金庫及び農業協同組合が大幅に減少。理由としては、警察の要請により、ほぼ全ての信用金庫及び農業協同組合でワンタイムパスワードが導入されたことが挙げられる。

(3)　不正アクセス禁止法違反の検挙件数等

○　不正アクセス禁止法違反の検挙人員は255人と引き続き増加。検挙件数は648件と過去５年では平成25年に次ぐ水準となった。

○　仮想通貨交換業者等への不正アクセスによる不正送信事犯認知件数は149件、被害額約６億6,240万円相当。

(4)　取組

○　官民連携によるウイルス感染を目的としたウェブサイト改ざんの対策

○　国際的な取組による流出ＩＤ等対策及び感染端末対策

○　自動送金機能を有するインターネットバンキングウイルス「DreamBot」に係る対策

○　一般財団法人日本サイバー犯罪対策センター（ＪＣ３）と連携したインターネットショッピングに係る詐欺サイト対策

○　被害防止に直結する情報の提供と被害防止対策強化の要請

３　今後の取組

「警察におけるサイバーセキュリティ戦略」（平成27年９月４日付け：警察庁乙官発第13号ほか）等を踏まえ、各種取組を推進する。

○　サイバー空間における情報収集・分析の推進

・　ダークウェブにおける情報収集の強化

○　官民連携の推進

・　ＪＣ３との連携

- サイバー空間の安全の確保に向けた情報の共有
- 連携した情報の発信による被害拡大防止対策

・　重要インフラ事業者、先端技術を有する事業者等との連携

・　二要素認証の促進

○　サイバー人材の育成

・　専門的捜査員の育成（CSセンター等における教育・訓練の拡充等）

・　情報技術の解析に係る高度専門人材の育成

○　国際連携

・　外国捜査機関との連携

○　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29年におけるサイバー空間をめぐる脅威の情勢等

１　サイバー攻撃の情勢等

(1)　サイバー空間における探索行為等

ア　センサー*1 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1,893.0件と引き続き増加している。

【図表１　センサーに対するアクセス件数の推移】

イ　特徴

○　ランサムウェア「WannaCry」の感染活動等

４月、「The Shadow Brokers」を名乗る集団により、Microsoft Windowsを標的とした攻撃ツール「Eternalblue」及び「Doublepulsar」が公開され、それ以降、当該攻撃ツールを悪用した感染機器の探索行為又は攻撃活動を観測した。

５月には、「Eternalblue」及び「Doublepulsar」を悪用して作成されたランサムウェア「WannaCry」が世界的に大流行し、警察庁においても、その感染活動を観測した。また、６月以降は、利用者に気付かれることなく感染する「WannaCry」の亜種が感染を拡大していることも確認した。

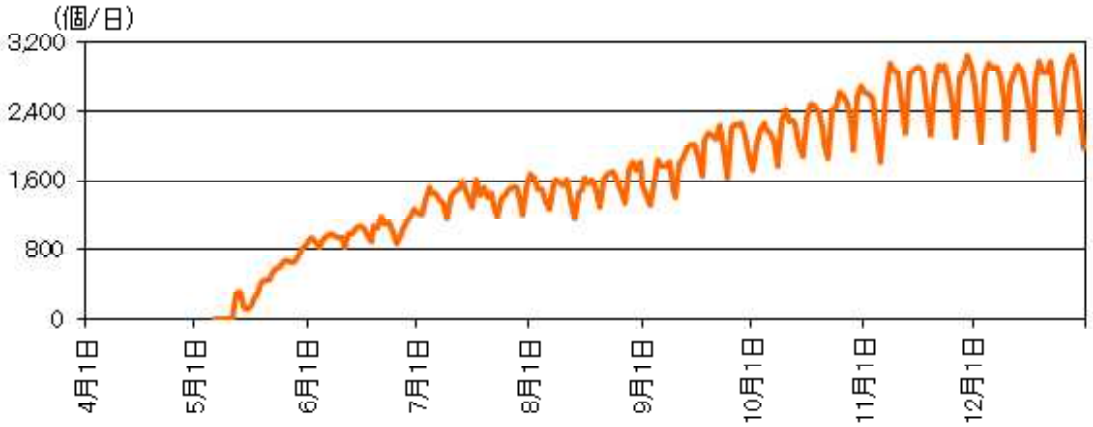
12月以降には、「Eternalblue」及び「Doublepulsar」を悪用した攻撃

---

*1　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。

活動とみられるアクセスの増加を観測した。

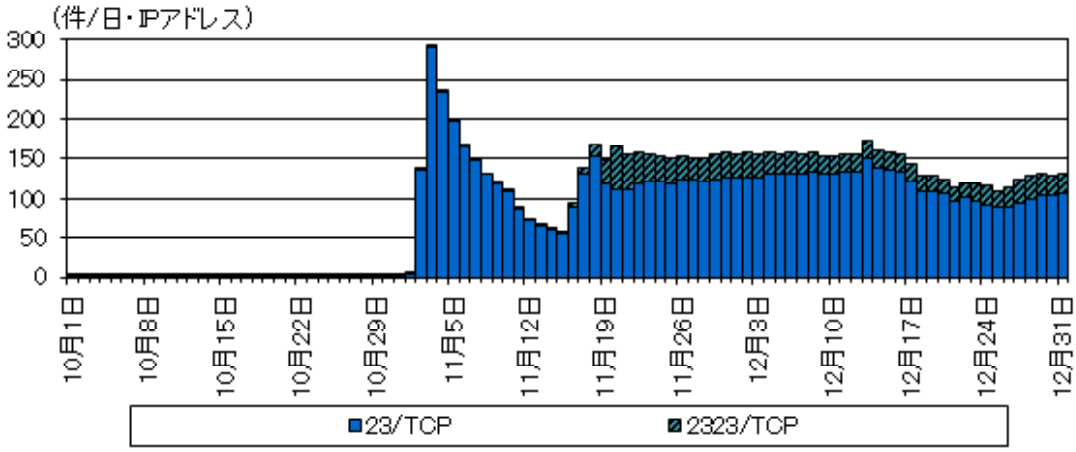
【図表２　WannaCryの感染活動の特徴を有するポート445/TCPに対するアクセスの発信元IPアドレス数の推移】



○　IoT機器を標的としたアクセス

11月以降、特定のルータに存在する脆弱性を標的とした感染活動とみられるアクセスの増加を観測した。また、同時期に、日本国内に割り当てられたIPアドレスを発信元とするIoT機器を標的とした探索行為又は感染活動とみられるアクセスの急増を観測した。

【図表３　日本国内からの宛先ポート23/TCP及び2323/TCPに対するアクセス件数の推移】



○　Apache Struts 2 [*2] 及び Apache Tomcat [*3] の脆弱性を標的としたアクセスの観測

Apache Struts 2 及び Apache Tomcat に存在する深刻な脆弱性を標的とした探索行為及び攻撃活動を観測した。

---

*2　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。

*3　Java言語でJavaサーブレット及びJSP（JavaServer Pages）と呼ばれる動的なウェブページを構築する際に使用されるソフトウェア（サーブレットコンテナ）。

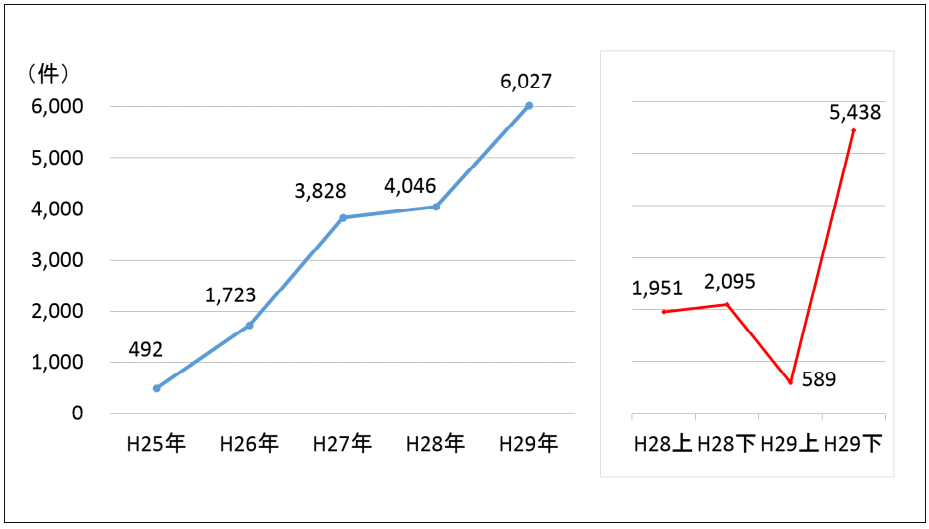
(2)　サイバー攻撃の情勢及び取組

ア　情勢

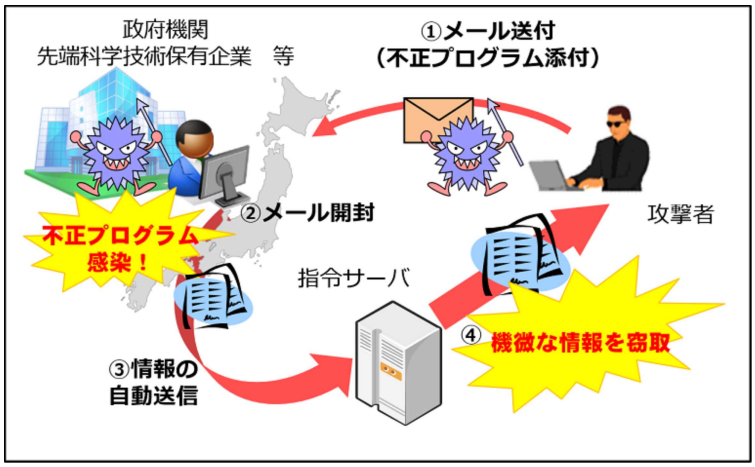
(ｱ)　概況

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*4 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把握した標的型メール攻撃の件数は6,027件と引き続き増加している。

【図表４　標的型メール攻撃の件数の推移】



【図表５　標的型メール攻撃の概要】



---

*4　警察と先端技術を有する全国7,737の事業者等（平成30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。

また、28年に引き続き、我が国の政府機関、公共交通機関、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、65組織に関して、サイバー攻撃を実行したとする犯行声明とみられる投稿を、SNS上に掲載している状況を把握している。

(ｲ) 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

28年から引き続き、「ばらまき型」攻撃[*5]が多数発生し、全体の97%を占めた。これらの中には、配送会社による再配達の連絡等を装い、大量に送信されていたものが確認された。

【図表６ 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	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)
28年中	90%（3,641件)	10%（ 405件)
29年中	97%（5,846件)	3%（ 181件)

○ 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90%を占め、過去数年と同様に、高い割合となった。

○ 多くの攻撃において送信元メールアドレスを偽装

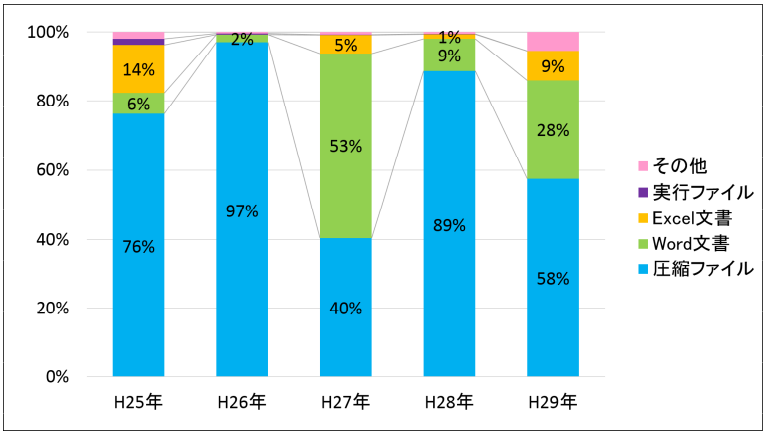
標的型メールの送信元メールアドレスについては、偽装されていると考えられるものが全体の62%を占めた。

*5 警察庁では、市販のウイルス対策ソフトでは検知できない不正プログラムを添付して、業務に関連した正当なものであるかのように装った電子メールを送信し、これを受信したコンピュータを不正プログラムに感染させるなどして、情報の窃取を図るものを「標的型メール攻撃」としているところ、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。

○　標的型メールに添付されたファイルの形式の割合の変化

標的型メールに添付されたファイルの形式の割合については、引き続き、圧縮ファイル、Word文書及びExcel文書が多数を占めた。Word文書が28年中の９％から28％に増加し、Excel文書が１％から９％に増加した。これらの中には、DDE機能[*6]を悪用したものやマクロ機能を悪用したものが確認された。

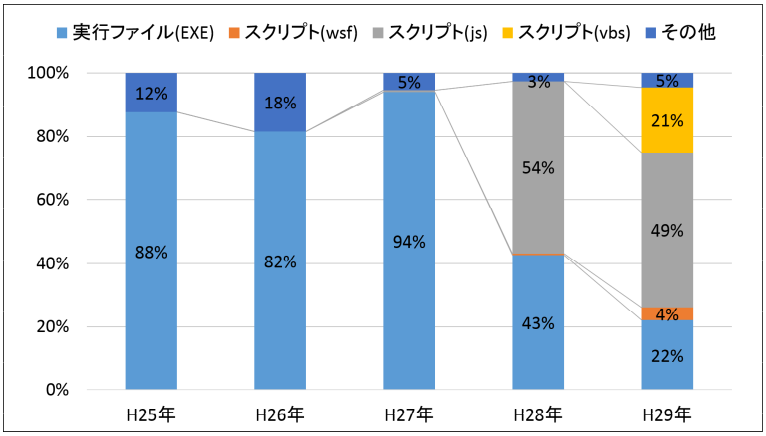
【図表７　標的型メールに添付されたファイル形式の割合】



○　圧縮ファイルで送付されたファイルの形式の変化

圧縮ファイルで送付されたファイルの形式については、25年から27年までは実行ファイルの割合が高かったが、28年にスクリプトファイル[*7]が確認され、29年はその割合が増加した。

【図表８　圧縮ファイルで送付されたファイル形式の推移】



*6　Dynamic Data Exchange（動的データ交換）の略。Windows環境においてアプリケーション間で通信を行う技術のこと。

*7　簡易的なプログラミング言語（スクリプト）で記述されたファイルのこと。不正な実行ファイルをダウンロードさせるために使用される場合がある。

イ　取組

(ｱ) 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[*8] の機能停止（テイクダウン）を、サーバを運営する事業者等に働きかけることで促進しており、29年中においては61台の機能停止が実施された。

(ｲ) 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攻撃対策の推進

2020年東京オリンピック・パラリンピック競技大会（以下「2020年東京大会」という。）に向けたサイバー攻撃対策として、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、大会開催国における関係機関等との情報交換等の取組を推進した。

【参考】2020年東京大会に向けた共同対処訓練の事例

○　平成29年６月、競技会場の東京スタジアムにおいて、サイバー攻撃による停電の発生や鉄道の運行停止等を想定した共同対処訓練を大会組織委員会及び重要インフラ事業者等と実施した。（警視庁）

○　平成29年12月、競技会場の幕張メッセにおいて、大規模イベント開催の警備中に、同イベントの妨害を企図するテロ組織が会場内に複数の爆発物を設置し、サイバー攻撃により会場内の照明・電源等の制御システムをダウンさせたという想定の共同対処訓練を実施した。（千葉県）

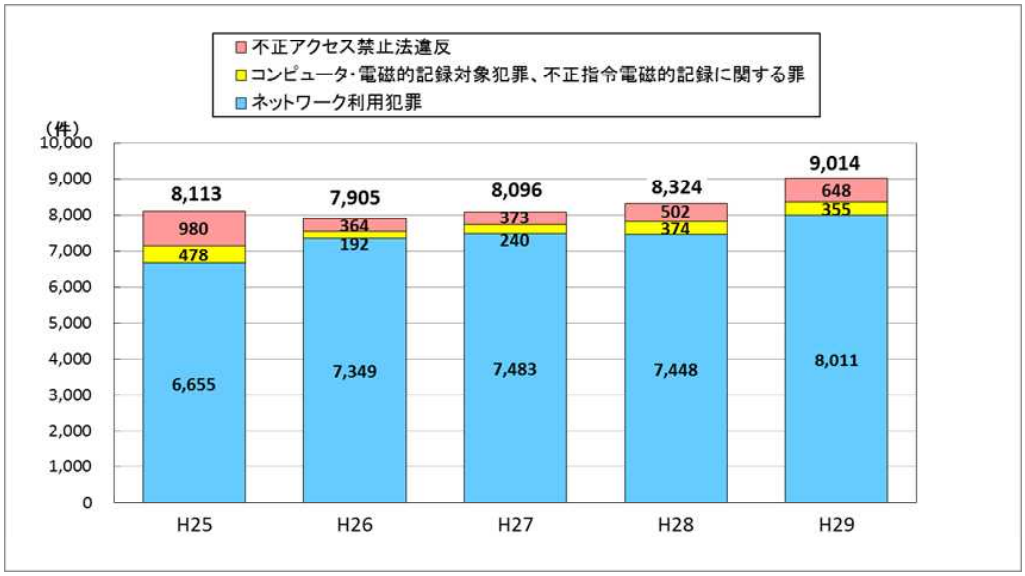
*8　Command and Control server（指令制御サーバ）の略。C&Cサーバと省略する場合もある。攻撃者の命令に基づいて動作する、不正プログラムに感染したコンピュータに指令を送り、制御の中心となるサーバのこと。

2　サイバー犯罪の情勢等

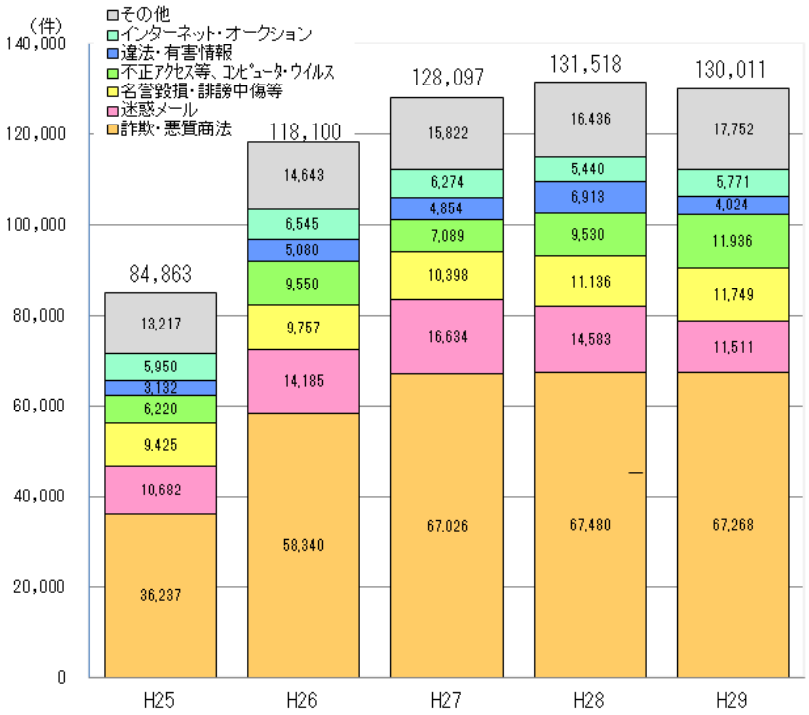
(1)　サイバー犯罪の検挙件数及びサイバー犯罪等に関する相談件数

サイバー犯罪の検挙件数は9,014件と引き続き増加している。相談件数は13万11件と引き続き高い水準にある。

【図表９　サイバー犯罪の検挙件数の推移】



【図表10　サイバー犯罪に関する相談件数の推移】



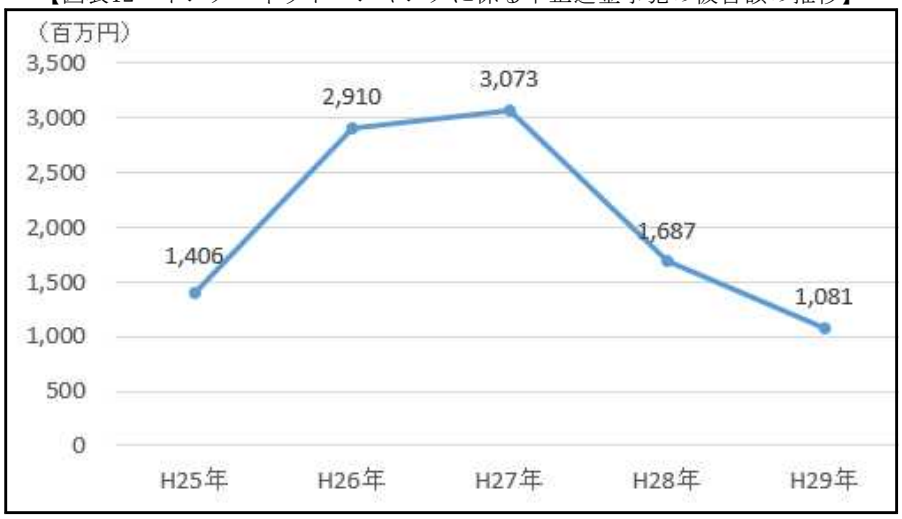
(2)　インターネットバンキングに係る不正送金事犯の発生状況等

ア　概況

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425件、被害額約10億8,100万円と、発生件数はピーク時の平成26年と比較して４分の１以下に減少、被害額はピーク時の平成27年と比較して約３分の１に減少した。

【図表11　インターネットバンキングに係る不正送金事犯の発生件数の推移】

【図表12　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の推移】



イ　特徴

○　都市銀行等の被害が大きく減少

モニタリング[*9] の強化、ワンタイムパスワードの導入等の対策により、都市銀行等を中心に近年被害が大幅に減少。

---

*9　不正送金に使用されたＩＰアドレス等に対する監視

○　電子決済サービスを用いた新たな手口による不正送金事犯が発生

被疑者が、インターネットバンキングに不正アクセスを行った後、電子決済サービスを使用して、あらかじめ用意しておいた仮想通貨交換業者のアカウントの円口座に、仮想通貨の購入資金として不正に送金を行う新たな手口による被害が約２億1,200万円発生した。

○　ワンタイムパスワードを聞き出す新たな手口による不正送金事犯が発生

ワンタイムパスワードを聞き出して送金を行う新たな手口による被害が約3,400万円発生した。

○　不正送金先口座はベトナム人名義のものが約６割

不正送金の一次送金先として把握した765口座のうち、名義人の国籍はベトナムが約59％を占め、次いで中国が約20％、日本が約12％を占めた。

ウ　関連事件の検挙

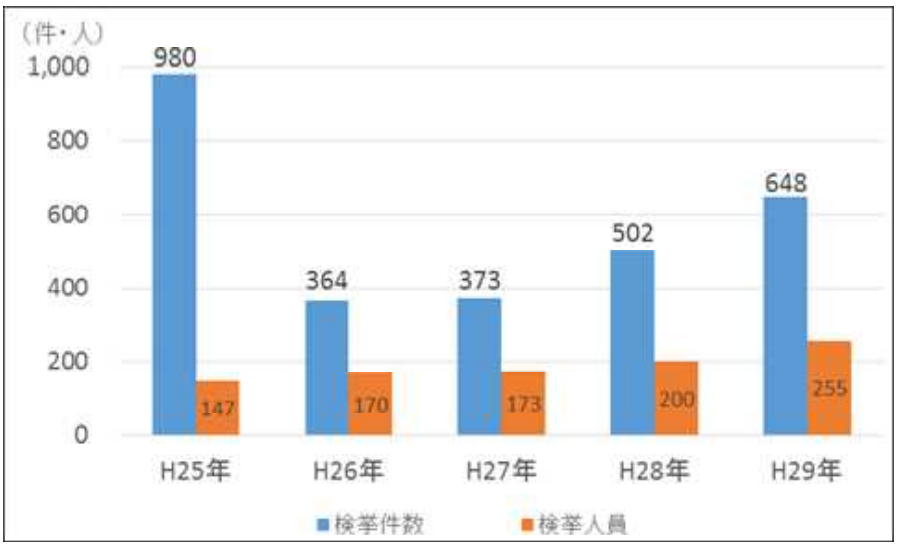
不正送金事犯に係る口座売買等の関連事件について、49事件・77人を検挙した。

(3)　不正アクセス禁止法違反の検挙状況等

ア　検挙状況

○　29年中の不正アクセス禁止法違反の検挙人員は255人と引き続き増加している。検挙件数は648件と、過去５年では平成25年に次ぐ水準となった。

【図表13　不正アクセス禁止法違反の検挙状況の推移】



○　違反行為別検挙件数では、不正アクセス行為が599件と最も多く、このうち545件が識別符号窃用型[*10]となっている。

○　不正アクセス行為の手口として「パスワード設定・管理の甘さにつけ込む手口」が最多

29年に検挙した識別符号窃用型の不正アクセス行為に係る手口の内訳は、利用権者のパスワードの設定・管理の甘さにつけ込んだものが230件と最も多く、次いで識別符号を知り得る立場にあった元従業員や知人等によるものが113件となっている。

○　不正に利用されたサービスとして「オンラインゲーム・コミュニティサイト」が最多

29年に検挙した識別符号窃用型の不正アクセス行為に係る被疑者に不正に利用されたサービスは、オンラインゲーム・コミュニティサイトが210件と最も多く、次いで社員・会員用等の専用サイトが116件、電子メールが92件となっている。

○　幅広い年齢層の被疑者等

不正アクセス禁止法違反で検挙又は補導された者は、13歳から60歳まで幅広い年齢層にわたっている。

イ　仮想通貨交換業者等への不正アクセスによる不正送信事犯

○　認知件数は149件、被害額約６億6,240万円相当。

○　仮想通貨交換業者等の多くでは、二要素認証[*11]を導入して利用者に利用を推奨しているものの、認知した149件のうち122件（81.9％）では、ＩＤ・パスワードによる認証のみしか使われていないなど、二要素認証を利用していなかった。

(4)　取組

○　官民連携によるウイルス感染を目的としたウェブサイト改ざんの対策

一般財団法人日本サイバー犯罪対策センター（ＪＣ３）からの情報提供

---

*10　アクセス制御されているサーバに、ネットワークを通じて、他人の識別符号を入力して不正に利用する行為

*11　人の認証に用いられる三つの要素（本人だけが知っていること、本人だけが所有しているもの及び本人自身の特徴）から二つの要素を組み合わせて用いる認証方式をいう。本人だけが知っているＩＤ・パスワードによる認証に本人だけが所有するスマートフォンアプリによる認証を追加する場合等がこれに当たる。

を元に、ＪＣ３と千葉県警察が連携して分析を行い、改ざん確認手法を確立し、全国38都道府県警察がサイト管理者に対して指導を行うなどの対策を実施した。

○　国際的な取組による流出ＩＤ等対策及び感染端末対策

ドイツ警察が中心となって行われた国際的な取組「オペレーションアバランチ」に関し、日本国内のインターネットバンキング利用者のＩＤ・パスワード等の情報、コンピュータウイルスの感染端末情報等を入手するに至ったことから、関係省庁・団体と連携して、インターネットバンキング利用者、感染端末利用者等に対し、被害拡大防止のための注意喚起を実施した。

○　自動送金機能を有するインターネットバンキングウイルス「DreamBot」に係る対策

不正送金ウイルス「DreamBot」に感染する被害の急増が確認されたことから、ＪＣ３と連携し、インターネット利用者や金融機関等に対して注意喚起を実施したほか、ＪＣ３がウェブサイト上に公開しているDreamBot感染チェックサイトの活用を促した。

○　ＪＣ３と連携したインターネットショッピングに係る詐欺サイト対策

ＪＣ３は、愛知県警察と共同で開発したツールの活用等により詐欺サイトを発見し、当該詐欺サイトのＵＲＬ情報をＡＰＷＧ[*12] 等に対し提供した。また、発見した国内の転送サイト（詐欺サイトに転送するよう改ざんされた正規サイト）については、県警察から当該正規サイトの管理者等に対し注意喚起を実施した。さらに、ＪＣ３からの情報に基づき、20都道府県警察が詐欺サイトにおいて利用された振込先の口座名義人等に対する取締りを実施した。

○　被害防止に直結する情報の提供と被害防止対策強化の要請

金融機関、電子決済運営管理団体、仮想通貨交換業者等に対して、モニタリングの強化、ワンタイムパスワードの利用促進、ログイン時の二経路

*12　Anti-Phishing Working Groupの略。フィッシングサイト対策を目的として平成15年に国際的な非営利団体として米国に設立。

認証[*13] の利用、本人確認の徹底等を要請した。

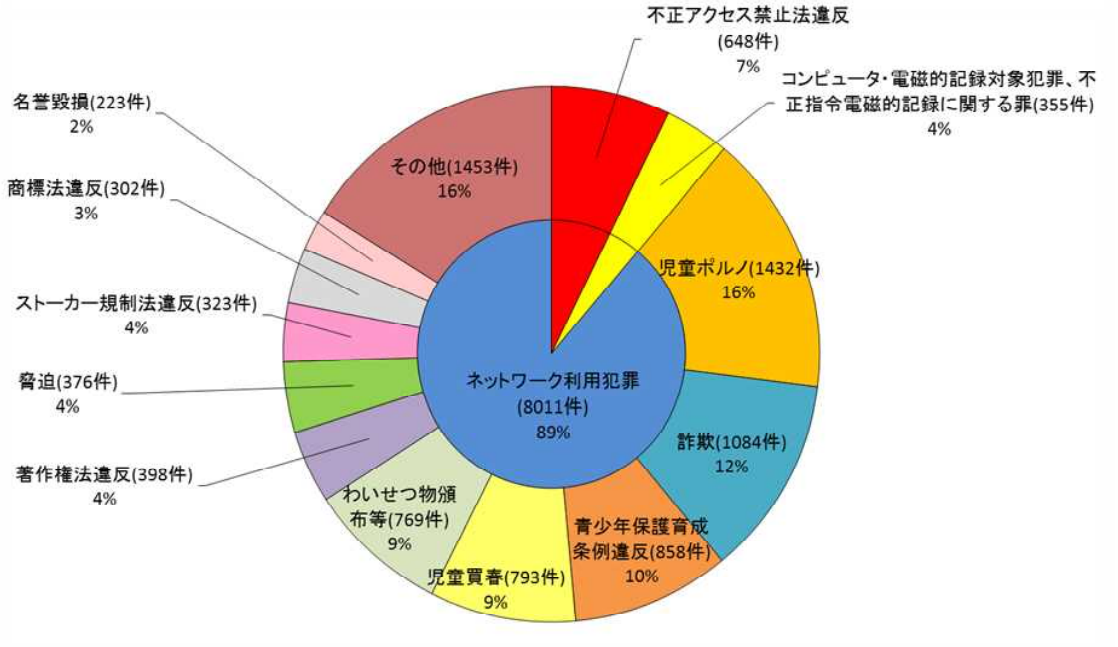
*13　振込データ等をパソコンで作成してスマートフォンで認証を行うなど、２つの経路で取引を成立させる認証方式のこと。仮にパソコンがコンピュータウイルス等に感染して不正な振込操作をされた場合でも、別経路（スマートフォン）での認証が必要となるため、不正利用を防止できる。

【　参考１　】

１　サイバー犯罪の検挙件数の内訳

罪名＼年	H25	H26	H27	H28	H29
不正アクセス禁止法違反	980	364	373	502	648
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	478	192	240	374	355
電子計算機使用詐欺	388	108	157	281	228
電磁的記録不正作出・毀棄等	56	48	32	24	39
電子計算機損壊等業務妨害	7	8	6	11	13
不正指令電磁的記録作成・提供	8	9	8	4	29
不正指令電磁的記録供用	14	16	21	36	24
不正指令電磁的記録取得・保管	5	3	16	18	22
ネットワーク利用犯罪	6,655	7,349	7,483	7,448	8,011
児童買春・児童ポルノ法違反（児童ポルノ）	1,124	1,248	1,295	1,368	1,432
詐欺	956	1,133	951	828	1,084
うちオークション利用詐欺	158	381	511	208	212
青少年保護育成条例違反	690	657	693	616	858
児童買春・児童ポルノ法違反（児童買春）	492	493	586	634	793
わいせつ物頒布等	781	840	835	819	769
著作権法違反	731	824	593	586	398
脅迫	189	313	398	387	376
ストーカー規制法違反	113	179	226	267	323
商標法違反	197	308	304	298	302
名誉毀損	122	148	192	215	223
その他	1,260	1,206	1,410	1,430	1,453
合　　計	8,113	7,905	8,096	8,324	9,014

２　ネットワーク利用犯罪の検挙状況の内訳



３　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】

○　高校生の少年（16）は、28年７月から同年10月までの間、他人のＩＤとパスワードを不正に取得するため、ＳＮＳサイト等を模したフィッシングサイトをインターネット上に公開し、当該サイトを閲覧した者にＩＤとパスワードを入力させてこれを取得した。29年６月、不正アクセス禁止法違反（識別符号の入力を不正に要求する行為等）で検挙した。（宮城・福井）

コンピュータ・電磁的記録対象犯罪

【私電磁的記録不正作出・同供用等】

○　無職の男（33）らは、29年２月、転売目的で作成することを秘して、フリーマーケットサイトのアカウントを大量に作成し販売した。29年６月、被疑者４名を私電磁的記録不正作出・同供用で検挙した。（山口・島根・鹿児島）

不正指令電磁的記録に関する罪

【不正指令電磁的記録取得】

○　少年（16）らは、29年３月、フリーマーケットサイトにおいて、コンピュータウイルスの入手方法を購入して同ウイルスを取得した。29年８月から同年９月にかけて、被疑者４名を不正指令電磁的記録取得で検挙した。（奈良）

ネットワーク利用犯罪

【詐欺】

○　仮想通貨運営会社代表社員の男（31）は、27年３月、顧客からの入金後に発行する電子借用証書が払出依頼によって確実に現金化できるものと誤信させ、同証書の発行を申し込んできた顧客から現金140万円を詐取した。29年10月、詐欺で検挙した。（警視庁）

【著作権法違反】

○　会社員の男（23）らは、28年３月から29年７月までの間、著作権者の許諾を受けないで、デジタル化した週刊漫画雑誌等のデータをサーバコンピュータに保存した上、運営するサイトに同データの保存先ＵＲＬを公開して、インターネットを利用する不特定多数の者が閲覧可能とした。29年10月、著作権法違反（公衆送信権の侵害）で検挙した。（大阪）

４　サイバー犯罪等に関する相談件数の内訳

	H25	H26	H27	H28	H29
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）	36,237	58,340	67,026	67,480	67,268
迷惑メールに関する相談	10,682	14,185	16,634	14,583	11,511
名誉毀損・誹謗中傷等に関する相談	9,425	9,757	10,398	11,136	11,749
不正アクセス等、コンピュータ・ウイルスに関する相談	6,220	9,550	7,089	9,530	11,936
違法・有害情報に関する相談	3,132	5,080	4,854	6,913	4,024
インターネット・オークションに関する相談	5,950	6,545	6,274	5,440	5,771
その他	13,217	14,643	15,822	16,436	17,752
合　計	84,863	118,100	128,097	131,518	130,011

５　相談事例

詐欺・悪質商法に関する相談

・　動画を閲覧しようとしたところ、登録料金を要求された。
・　ネットショップで商品を注文したが届かない。

迷惑メールに関する相談

・　「寄付してくださいました件で今から集金に伺います。」というメール

が送られてきた。
・　「このたび当選まことにおめでとうございます。１億円が当選していますので、表示されたＵＲＬに接続して確認してください。」というメールが送られてきた。

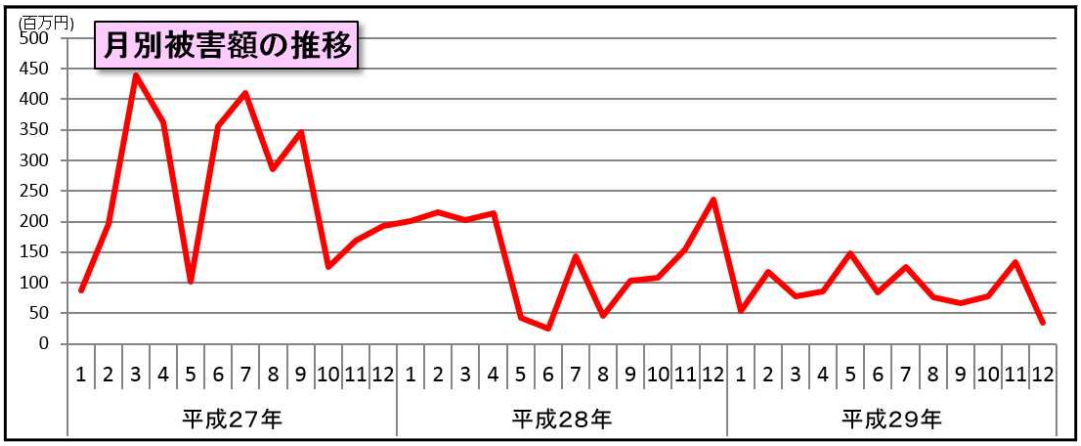
名誉毀損・誹謗中傷等に関する相談
・　掲示板サイトに個人情報を掲載されて、誹謗中傷する内容を書き込まれた。

不正アクセス等、コンピュータ・ウイルスに関する相談
・　ウイルス感染を警告する画面が表示され、画面に表示されていた電話番号に電話するとウイルス駆除料金を要求された。
・　仮想通貨交換業者に不正アクセスされ、仮想通貨をとられた。

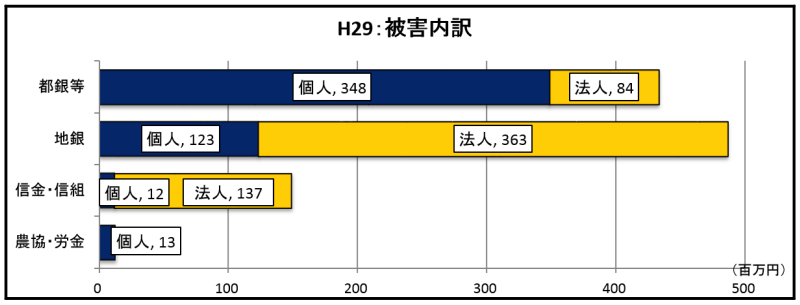
【　参考２　】

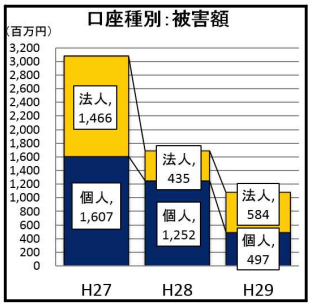
インターネットバンキングに係る不正送金事犯の発生状況

(1) 発生状況の推移



(2) 被害内訳

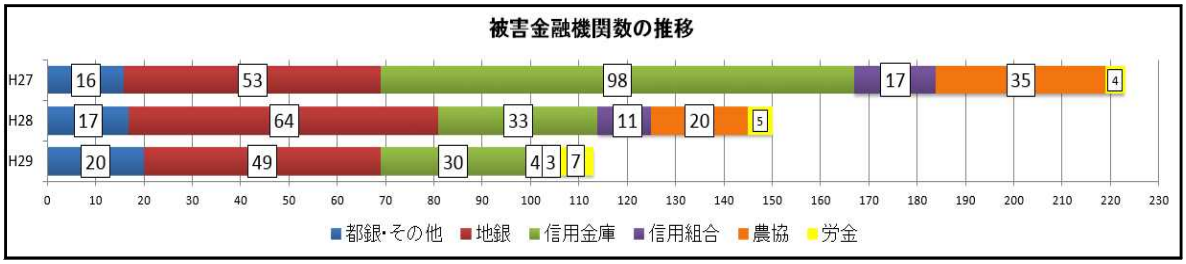




(3) 被害金融機関

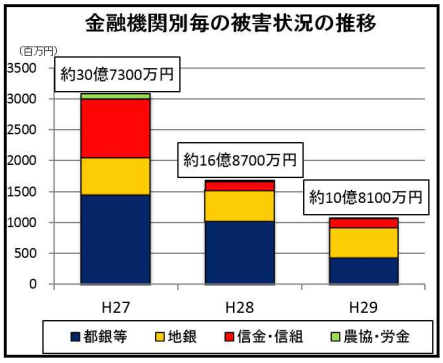
１１３金融機関

都市銀行・信託銀行・ネット専業銀行・その他の銀行	２０行
地方銀行	４９行
信用金庫	３０金庫
信用組合	４組合
農業協同組合	３組合
労働金庫	７金庫



(4) 金融機関別毎の被害状況

金融機関別	H27	H28	H29
都銀等	約14億4600万円	約10億2500万円	約4億3300万円
地　銀	約6億円	約4億9500万円	約4億8600万円
信金・信組	約9億4000万円	約1億4500万円	約1億4900万円
農協・労金	約8700万円	約2100万円	約1300万円
合　計	約30億7300万円	約16億8700万円	約10億8100万円

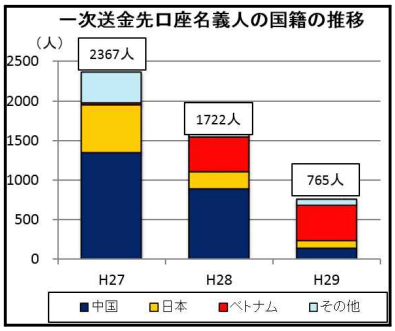


(5) 口座種別毎の被害状況

口座種別		平成29年				
		都市銀行等	地方銀行	信金・信組	農協・労金	合計
個人	被害額	約3億4800万円 (32.2%)	約1億2300万円 (11.4%)	約1200万円 (1.1%)	約1300万円 (1.2%)	約4億9700万円 (46.0%)
	実被害額	約2億9100万円 (32.4%)	約1億1400万円 (12.7%)	約1000万円 (1.1%)	約1200万円 (1.3%)	約4億2800万円 (47.5%)
法人	被害額	約8400万円 (7.8%)	約3億6300万円 (33.6%)	約1億3700万円 (12.6%)		約5億8400万円 (54.0%)
	実被害額	約7700万円 (8.6%)	約2億7200万円 (30.2%)	約1億2300万円 (13.7%)		約4億7200万円 (52.5%)
合計	被害額	約4億3300万円 (40.0%)	約4億8600億円 (45.0%)	約1億4900万円 (13.8%)	約1300万円 (1.2%)	約10億8100万円 (100.0%)
	実被害額	約3億6800万円 (40.9%)	約3億8600万円 (42.9%)	約1億3300万円 (14.8%)	約1200万円 (1.3%)	約8億9900円 (100.0%)

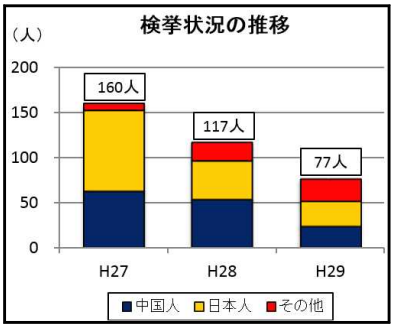
(6) 一次送金先口座名義人の国籍

	H27		H28		H29	
中　国	1,350	57.0%	892	51.8%	151	19.7%
日　本	603	25.5%	219	12.7%	89	11.6%
ベトナム	25	1.1%	438	25.4%	452	59.1%
その他	389	16.4%	173	10.0%	73	9.5%
合　計	2,367	100.0%	1,722	100.0%	765	100.0%



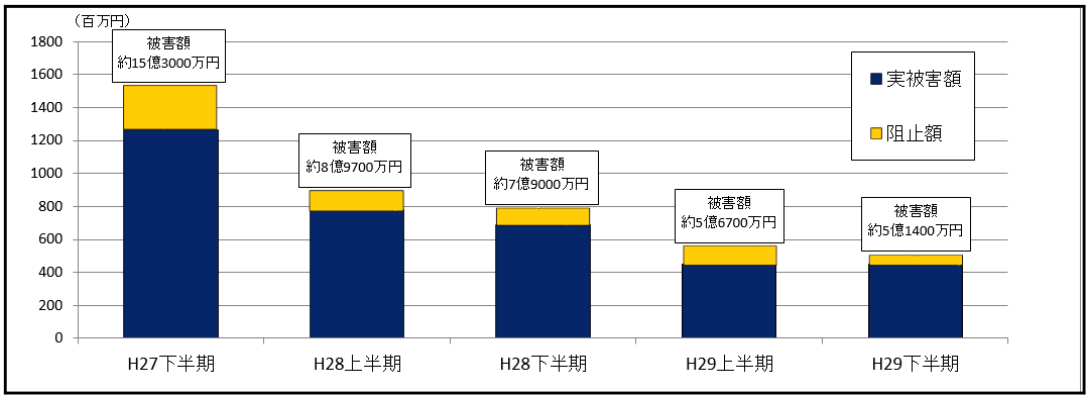
(7) 関連事件の検挙状況

		H27		H28		H29	
検挙事件		97件		75件		49件	
検挙人数		160人		117人		77人	
内訳	中国人	63人	39.4%	53人	45.3%	24人	31.2%
	日本人	90人	56.3%	44人	37.6%	28人	36.4%
	その他	7人	4.4%	20人	17.1%	25人	32.5%



(8) 不正送金阻止状況

	被害額	実被害額	阻止額	阻止率
H27下半期	約15億3000万円	約12億6400万円	約2億6600万円	17.4%
H28上半期	約8億9700万円	約7億7600万円	約1億2000万円	13.4%
H28下半期	約7億9000万円	約6億8700万円	約1億400万円	13.2%
H29上半期	約5億6700万円	約4億5000万円	約1億1800万円	20.8%
H29下半期	約5億1400万円	約4億5000万円	約6400万円	12.5%



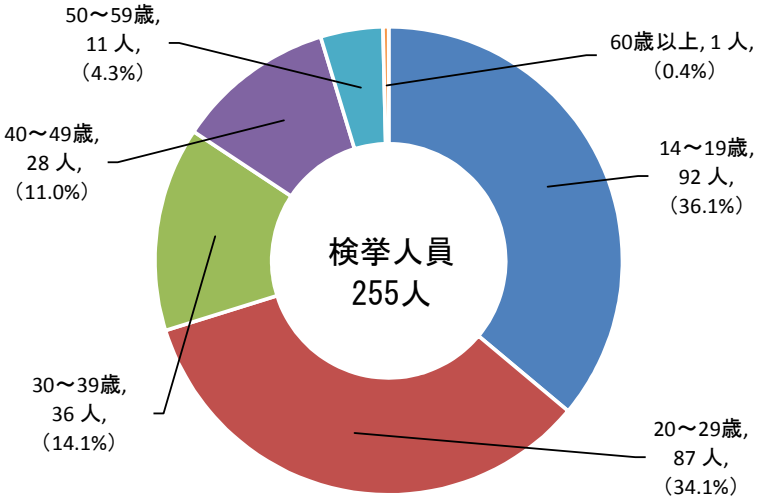
(9) 不正送金被害に係る口座名義人のセキュリティ対策実施状況

	利用していた		利用していない		不　明		合　計
ワンタイムパスワード（個人口座）	115	35.2%	194	59.3%	18	5.5%	327
電子証明書（法人口座）	35	35.7%	62	63.3%	1	1.0%	98

【　参考３　】

不正アクセス禁止法違反の検挙状況等

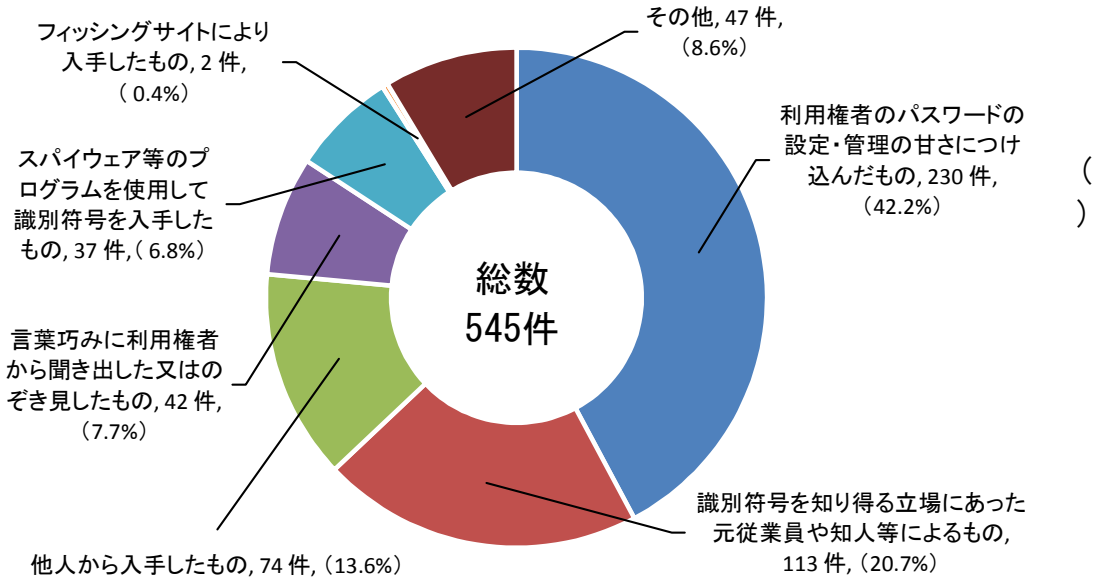
(1) 年代別被疑者数



※　このほか、不正アクセス禁止法違反により、14歳未満の少年２名が触法少年として補導されている。

(2) 不正アクセス行為（識別符号窃用型[*10]）に係る手口別検挙件数

3



*10　アクセス制御されているサーバに、ネットワークを通じて、他人の識別符号を入力して不正に利用する行為

(3) 不正に利用されたサービス別検挙件数（識別符号窃用型）