広　報　資　料
平成30年９月20日
警　　察　　庁

平成30年上半期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おいて検知したアクセス件数は、１日１IP アドレス当たり2,223.6件と近年おおむね増加傾向。

○　アクセス件数が増加している主な要因としては、探索又は攻撃の標的がIoT機器等へ拡大し多様化が進んでいることなどが挙げられる。

○　仮想通貨のネットワーク等を標的としたアクセスや、仮想通貨の採掘機能を備えた不正プログラムの感染活動等を観測。

(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の件数は近年増加傾向にある中、本年上半期の件数（2,578件）は過去最多となった前年下半期と比較して減少。

○　国際的ハッカー集団「アノニマス」を名乗る者が、15組織に対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近年増加傾向にある中、本年上半期の件数（4,183件）は過去最多となった前年の上半期と比較して微減。また、相談件数は平成28年に集計をとり始めて以来最多を記録したが、平成29年には減少し、本年上半期の件数（６万1,473件）も前年の上半期と比較し

て減少。

(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211件、被害額は約３億7,200万円で、いずれも減少傾向

○　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、被害件数・被害額共に大きく減少。

(3)　仮想通貨交換業者等への不正アクセス等による不正送信事犯

○　認知件数158件（前年同期比＋107件）、被害額約605億300万円（前年同期比＋約603億8,800万円）相当。認知した158件のうち102件（64.6％）において、利用者が他のインターネット上のサービスと同一のID・パスワードを使用。

○　本年１月、国内の仮想通貨交換業者から約580億円相当の仮想通貨が不正に送信されたとみられる事案が発生。

(4)　取組

○　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」に係る対策及びインターネットショッピングに係る詐欺サイト対策。

○　仮想通貨不正送信事犯に係る対策として、金融庁に対し、同事犯の認知状況等についての情報提供と仮想通貨交換業者に対する指導等への協力・支援を確認。

○　被害防止のための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」に基づく各種取組の推進

○　サイバー空間の脅威への対応の強化

・　サイバー犯罪に対する捜査の推進、情報技術の解析の更なる活用

・　サイバー攻撃に関する情報の収集・分析、重要インフラ事業者等との情報共有、捜査及び実態解明等の推進

・　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）

○　組織基盤の更なる強化

・　専門的捜査員の計画的な育成、情報技術の解析に係る高度専門人材の育成

・　人工知能（AI）等の新たな技術の活用、ダークウェブ上の情報の収集・分析手法等の研究開発

○　国際連携及び産学官連携の推進

・　外国捜査機関等との連携

・　ＪＣ３等と連携した被害防止対策等の推進

別　添

平成30年上半期におけるサイバー空間をめぐる脅威の情勢等

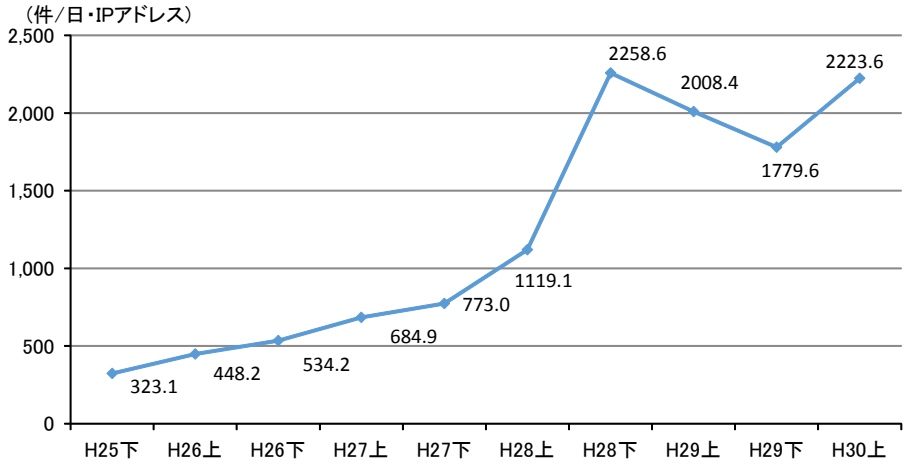
1　サイバー攻撃の情勢等

(1)　サイバー空間における探索行為等

ア　センサー[*1] において検知したアクセスの概況

センサーにおいて検知したアクセス件数は、１日・１IPアドレス当たり2,223.6件と近年おおむね増加傾向にある。

【図表１　センサーにおいて検知したアクセス件数の推移】



イ　特徴

○　攻撃や探索の標的が多様化

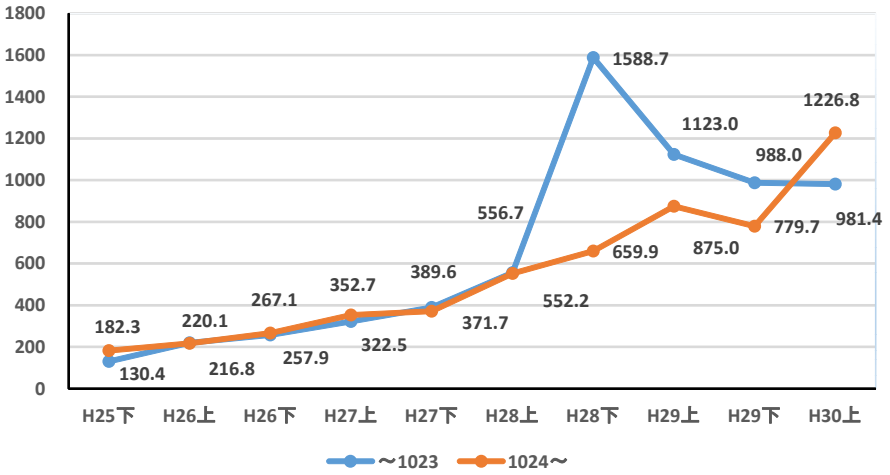
検知したアクセスの宛先ポート[*2] に着目すると、一般に広く利用されているポート（1023以下のポート）に対するアクセスについては、引き続き高い水準にあるものの、平成29年上半期からは減少傾向に転じた。一方、IoT機器や特定の相手との通信等に利用されているポート（1024以上のポート）に対するアクセスは増加傾向にあり、30年上半期においては、同ポートに対する１日・１IPアドレス当たりのアクセスの件数は、1023以下のポートに対するものの件数を上回った。

---

*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。

*2　ポートとは、TCP/IP通信において、通信を行うコンピュータが、どのプログラムを通信に使用するのかを識別するためのインターフェースで、０から65535までの番号が割り当てられている。

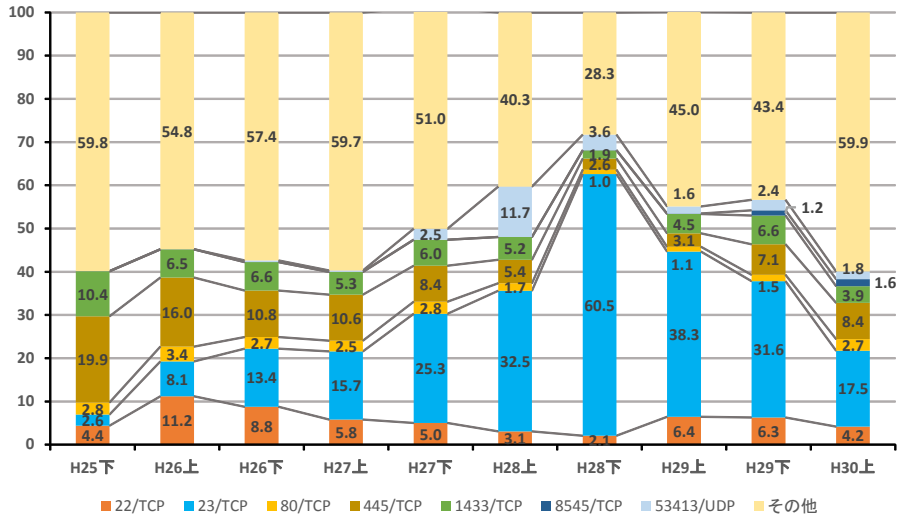
【図表２　検知したアクセスの宛先ポートで比較した１日・１IPアドレス当たり件数の推移】



また、平成30年上半期において検知したアクセスの宛先ポート別の比率については、「その他」の比率が増加し、特定ポートに集中したアクセスの比率は減少しているが、その原因は、探索又は攻撃の標的が、IoT機器や仮想通貨のネットワーク等へ拡大するなど多様化が進んでいることが考えられる。

その他の特徴としては、Miraiボットからのものと見られる宛先ポート80/TCPに対するアクセスや、Microsoft Windowsの脆弱性を標的とした宛先ポート445/TCPに対するアクセスの割合が再び増加している。

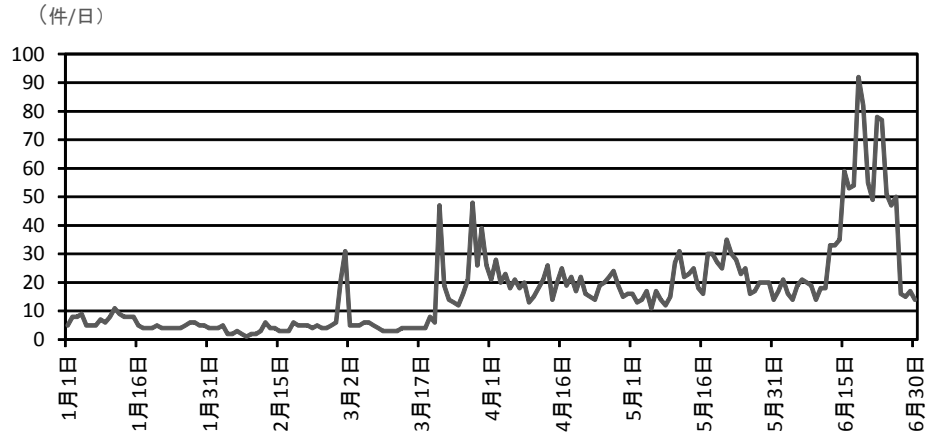
【図表３　検知したアクセスの宛先ポート別の比率の推移】



○　仮想通貨のネットワーク等を標的としたアクセスの観測

近年、仮想通貨のネットワーク等を標的としたアクセスが増加しており、30年３月下旬以降、「Ethereum」のネットワークを標的としているとみられるアクセスの発信元IPアドレス数の増加を観測し、同年６月中旬には、その急増を観測した。

【図表４　「Ethereum」のネットワークを標的としているとみられる宛先ポート8545/TCPに対するアクセスの発信元IPアドレス数の推移】

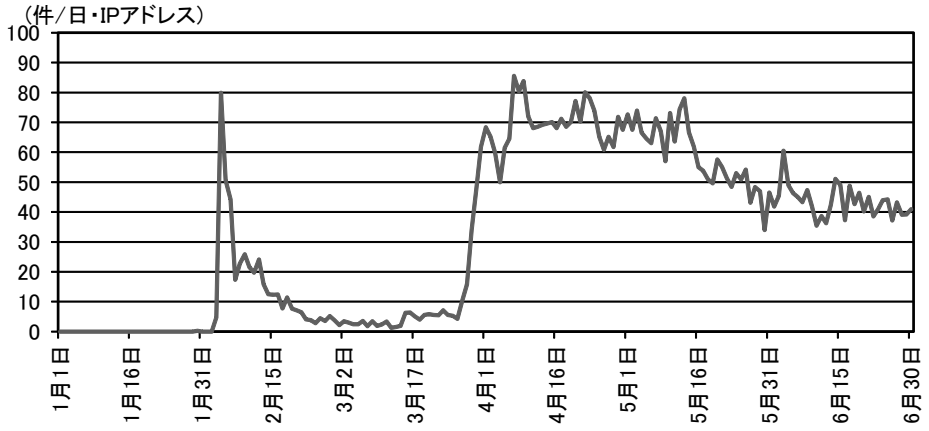


また、30年１月以降、仮想通貨「Ethereum」の採掘ソフトウェア「Claymore」を標的としたアクセスを、同年５月下旬以降は、仮想通貨「EOS」を標的とした探索行為と見られるアクセスの増加を観測した。

○　仮想通貨の採掘機能等を備えた不正プログラムの感染活動等

30年２月には、Android TV BOX等の端末に感染して仮想通貨を無断で採掘する不正プログラム「ADB.Miner」によるものと考えられるアクセスの増加を観測したところ、同年３月下旬以降、多数のアクセスを観測した。

【図表５　Android TV BOX等の端末を標的にしているとみられる宛先ポート5555/TCPに対するアクセス件数の推移】



このほか、同年３月下旬以降は、脆弱性を有していたNoSQLデータベース「Redis」、コンテンツ管理システム「Drupal」及びGPONルータ等を標的としたアクセスを観測した。

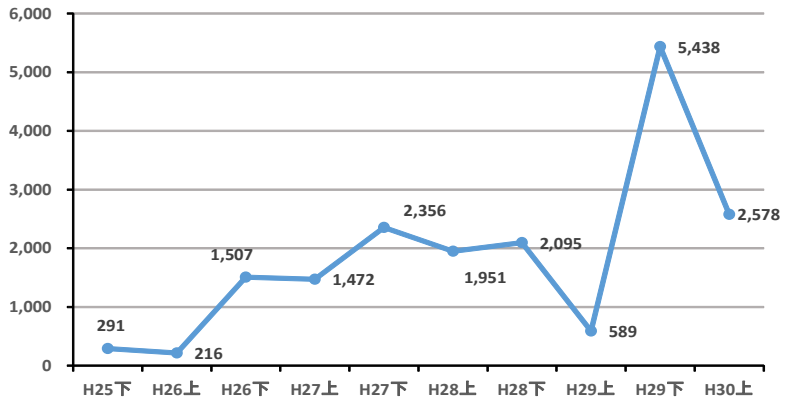
(2)　サイバー攻撃の情勢及び取組

ア　情勢

(ｱ)　概況

警察では、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、サイバーインテリジェンス情報共有ネットワーク[*3]により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近年増加傾向にある中、本年上半期の件数（2,578件）は過去最多となった前年下半期と比較して減少した。

【図表６　標的型メール攻撃の件数の推移】

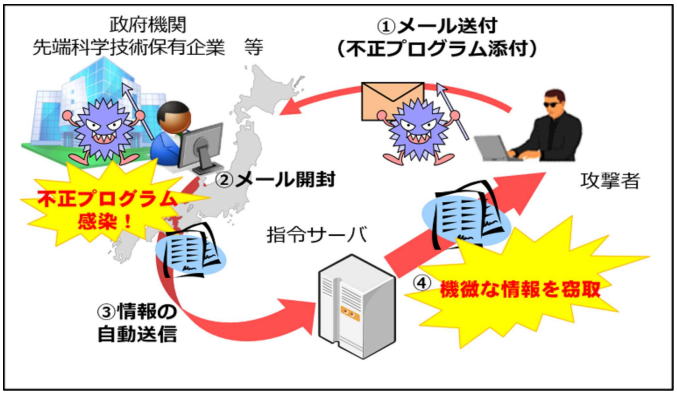


また、29年に引き続き、我が国の行政機関、公共交通機関、博物館等のウェブサイトに閲覧障害が生じる事案が発生した。

警察では、国際的ハッカー集団「アノニマス」を名乗る者が、15組織に対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

【図表７　標的型メール攻撃の概要】



---

*3　警察と先端技術を有する全国7,769の事業者等（30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。

○　「ばらまき型」攻撃の多発傾向が継続

「ばらまき型」攻撃[*4]が多数発生し、全体の87%を占め、引き続き高い割合となった。

【図表８　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
H25下	63.6%　（　185件）	36.4%　（106件）
H26上	39.8%　（　86件）	60.2%　（130件）
H26下	92.1%　（1,388件）	7.9%　（119件）
H27上	91.5%　（1,347件）	8.5%　（125件）
H27下	91.7%　（2,161件）	8.3%　（195件）
H28上	85.4%　（1,667件）	14.6%　（284件）
H28下	94.2%　（1,974件）	5.8%　（121件）
H29上	89.0%　（　524件）	11.0%　（　65件）
H29下	97.9%　（5,322件）	2.1%　（116件）
H30上	87.1%　（2,246件）	12.9%　（332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85%を占め、引き続き高い割合となった。

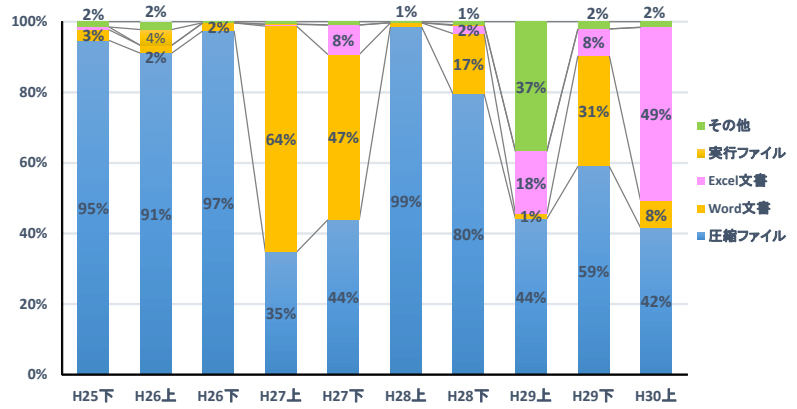
○　多くの攻撃において送信元メールアドレスを偽装

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96%を占めた。

○　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については、平成30年上半期はExcel文書の占める割合が大幅に増加した。

【図表９　標的型メールに添付されたファイルの形式の割合】

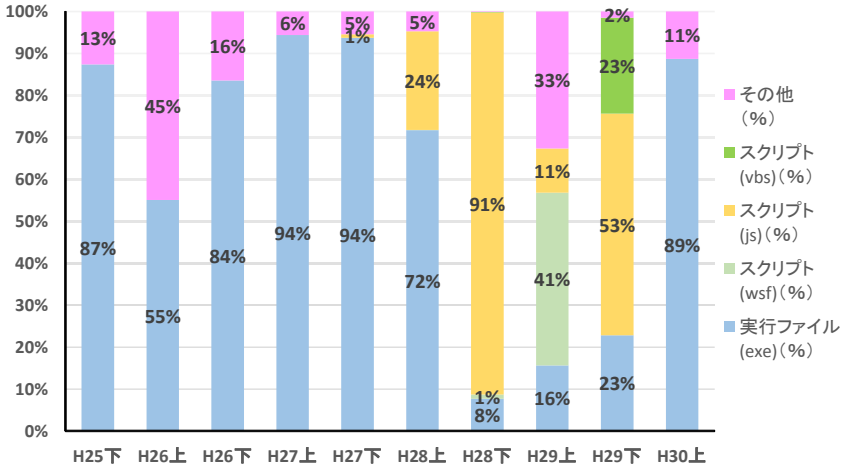


*4　警察庁では、市販のウイルス対策ソフトでは検知できない不正プログラムを添付して、業務に関連した正当なものであるかのように装った電子メールを送信し、これを受信したコンピュータを不正プログラムに感染させるなどして、情報の窃取を図るものを「標的型メール攻撃」としているところ、同じ文面や不正プログラムが10か所以上に送付されていた標的型メール攻撃を「ばらまき型」として集計している。

○　圧縮ファイルで送付されたファイルの形式の割合の変化

圧縮ファイルで送付されたファイルの形式については、28年下半期から高い割合を占めていたスクリプトファイル[*5]が確認されず、実行ファイルが高い割合を占めた。

【図表10　圧縮ファイルで送付されたファイル形式の推移】



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[*6]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、30年上半期においては６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。

---

*5　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。

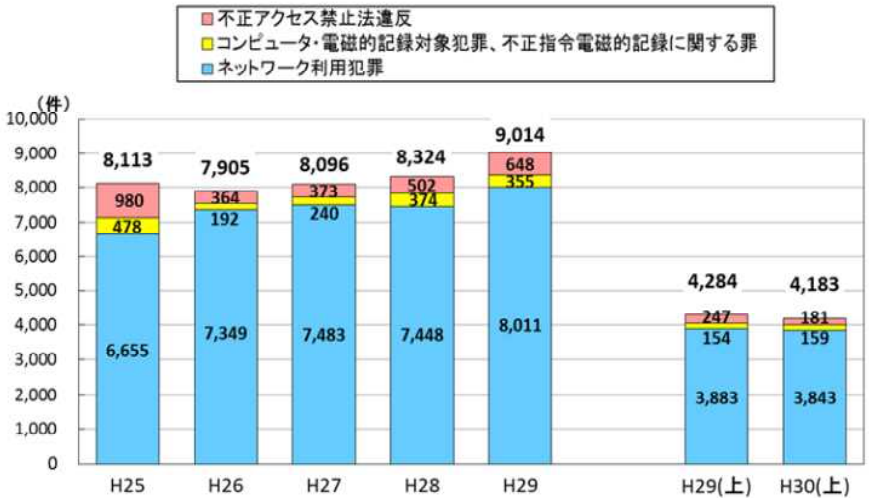
*6　Command and Control server（指令制御サーバ）の略。C&Cサーバと省略する場合もある。攻撃者の命令に基づいて動作する、不正プログラムに感染したコンピュータに指令を送り、制御の中心となるサーバのこと。

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

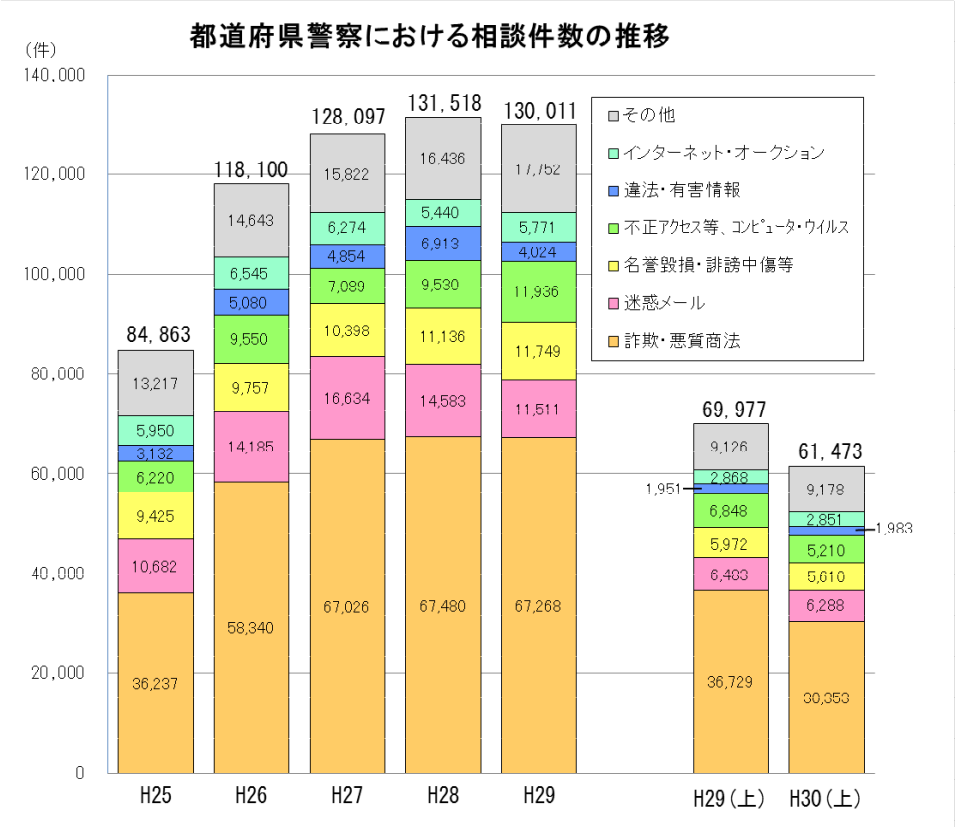
サイバー犯罪の検挙件数は近年増加傾向にある中、本年上半期の件数（4,183件）は過去最多となった前年の上半期と比較して微減となった。また、相談件数は平成28年に集計をとり始めて以来最多を記録したが、平成29年には減少し、本年上半期の件数（６万1,473件）も前年上半期と比較して減少した。

【図表11　サイバー犯罪の検挙件数の推移】



※H30(上)は暫定値

【図表12　サイバー犯罪に関する相談件数の推移】

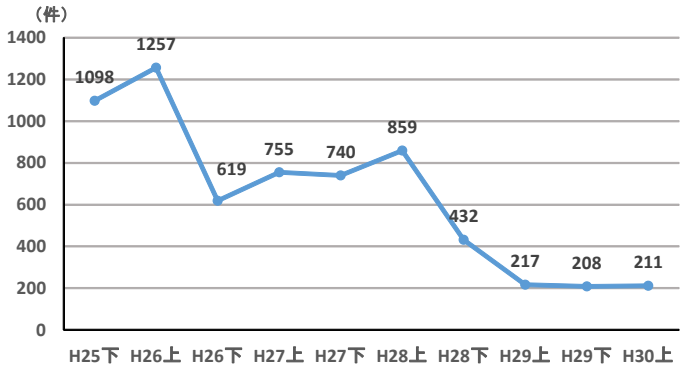


(2)　インターネットバンキングに係る不正送金事犯の発生状況等

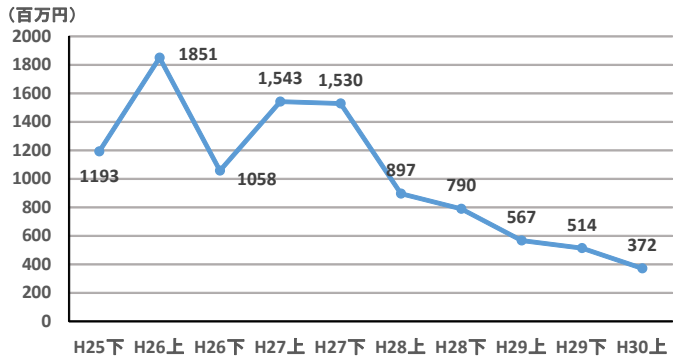
ア　概況

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211件、被害額約３億7,200万円で、いずれもおおむね減少傾向にある。

【図表13　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14　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

○　法人口座の被害が大きく減少

モニタリング*7 の強化、ワンタイムパスワードの導入等の対策により、29年上半期と比較して、地方銀行・信用金庫等を中心に法人口座の被害が減少した。

○　電子決済サービスを用いた不正送金事犯が大きく減少

電子決済サービスを用いた不正送金事犯は、仮想通貨の購入資金として不正に送金を行う手口の発生がなく、全体で大きく減少した。

○　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358口座のうち、名義人の国籍はベトナムが約65％を占め、次いで中国が約15％、日本が約12％であった。

---

*7　不正送金に使用されたＩＰアドレス等に対する監視

(3)　仮想通貨交換業者等への不正アクセス等による不正送信事犯

○　認知件数は158件、被害額は約605億300万円相当で、29年上半期（認知件数51件、被害額１億1,500万円相当）と比較して、認知件数は107件、被害額は約603億8,800万円相当上回った。

本年１月には、国内の仮想通貨交換業者から約580億円相当の仮想通貨が不正に送信されたとみられる事案が発生した。

○　認知した158件のうち102件（64.6％）では、利用者が、ID・パスワードを他のインターネット上のサービスと同一にしていた。

(4)　取組

○　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」に感染する被害が続いていることから、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、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ているほか、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ている。

○　仮想通貨不正送信事犯に係る対策

金融庁に対して、仮想通貨不正送信事犯の認知状況等について情報提供を行うとともに、仮想通貨交換業者に対する指導等への協力・支援を確認した。

○　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[*8] 等に対し提供している。

○　被害防止のための情報の提供と被害防止対策強化の要請

金融機関等に対して、モニタリングの強化、ワンタイムパスワード及びログイン時の二経路認証[*9] の利用促進、本人確認の徹底等を働き掛けた。

---

*8　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。

*9　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。

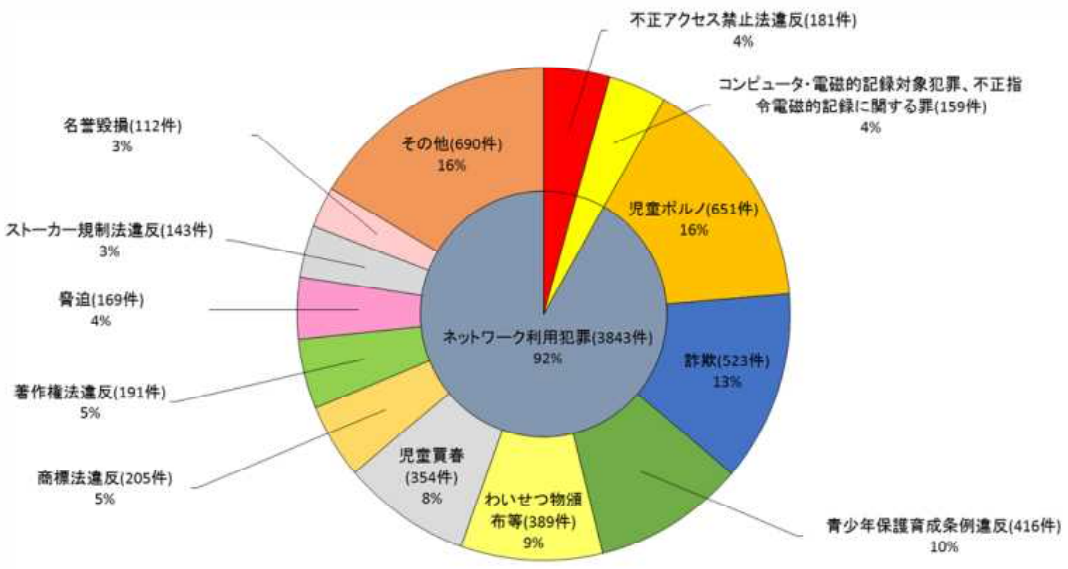
【　参考１　】

１　サイバー犯罪の検挙件数の内訳

罪名＼年	H25	H26	H27	H28	H29	H29（上）	H30（上）
不正アクセス禁止法違反	980	364	373	502	648	247	181
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	154	159
電子計算機使用詐欺	388	108	157	281	228	103	88
電磁的記録不正作出・毀棄等	56	48	32	24	39	20	33
電子計算機損壊等業務妨害	7	8	6	11	13	9	2
不正指令電磁的記録作成・提供	8	9	8	4	29	3	6
不正指令電磁的記録供用	14	16	21	36	24	14	16
不正指令電磁的記録取得・保管	5	3	16	18	22	5	14
ネットワーク利用犯罪	6,655	7,349	7,483	7,448	8,011	3,883	3,843
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	725	651
詐欺	956	1,133	951	828	1,084	505	523
うちオークション利用詐欺	158	381	511	208	212	140	68
青少年保護育成条例違反	690	657	693	616	858	396	416
わいせつ物頒布等	781	840	835	819	769	391	389
児童買春・児童ポルノ法違反（児童買春）	492	493	586	634	793	385	354
商標法違反	197	308	304	298	302	156	205
著作権法違反	731	824	593	586	398	189	191
脅迫	189	313	398	387	376	216	169
ストーカー規制法違反	113	179	226	267	323	166	143
名誉毀損	122	148	192	215	223	115	112
その他	1,260	1,206	1,410	1,430	1,453	639	690
合　計	8,113	7,905	8,096	8,324	9,014	4,284	4,183

※H30（上）は暫定値

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】

○　無職の男（21）は、29年６月、掲示板サイトから不正に入手したＩＤ・パスワードのリストを使用して、国内のオークションサイト等へ不正アクセスした。30年２月、不正アクセス禁止法違反（不正アクセス行為）で検挙した。（和歌山）

コンピュータ・電磁的記録対象犯罪

【電子計算機使用詐欺】

○　自営業の男（37）は、29年７月、宿泊予約サイト運営会社に対し、不正に入手したクレジットカード情報を利用してカード決済をして、宿泊料金の支払いを免れた。30年１月、電子計算機使用詐欺で検挙した。（千葉・茨城・栃木）

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罪】

○　無職の男（22）は、29年８月、保有する記録媒体に身代金要求型ウイルスであるランサムウェアを保管した。30年２月、不正指令電磁的記録保管で検挙した。（香川）

ネットワーク利用犯罪

【詐欺】

○　自営業の男（44）らは、29年11月、真実はコンサートに参加する意思はなく、チケットを営利目的で第三者に転売する意思であるのに、これを秘して、チケット配給会社からチケットを詐取した。30年１月、詐欺で検挙した。（兵庫）

【著作権法違反】

○　会社員の男(42)は、29年７月から10月までの間、著作権者の許諾を受けないで、ゲームソフトを複製した記録媒体を国内のオークションサイトで販売した。30年２月、著作権法違反（権利侵害品の頒布）で検挙した。（島根）

４　サイバー犯罪等に関する相談件数の内訳

	H25	H26	H27	H28	H29	H29（上）	H30（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）	36,237	58,340	67,026	67,480	67,268	36,729	30,353
迷惑メールに関する相談	10,682	14,185	16,634	14,583	11,511	6,483	6,288
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	5,972	5,610
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	6,848	5,210
違法・有害情報に関する相談	3,132	5,080	4,854	6,913	4,024	1,951	1,983
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	2,868	2,851
その他	13,217	14,643	15,822	16,436	17,752	9,126	9,178
合　　計	84,863	118,100	128,097	131,518	130,011	69,977	61,473

５　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サイトで商品を注文し、代金を支払ったが商品が届かない。
- 取引先を騙る者からメールで商品代金振込方法変更を指示され、振込を行ってしまった。
- インターネットショッピングサイトを騙る者から「料金未納が発生しています。」という内容のメールが送られてきた。

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。

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るとともに誹謗中傷する内容を書き込まれた。

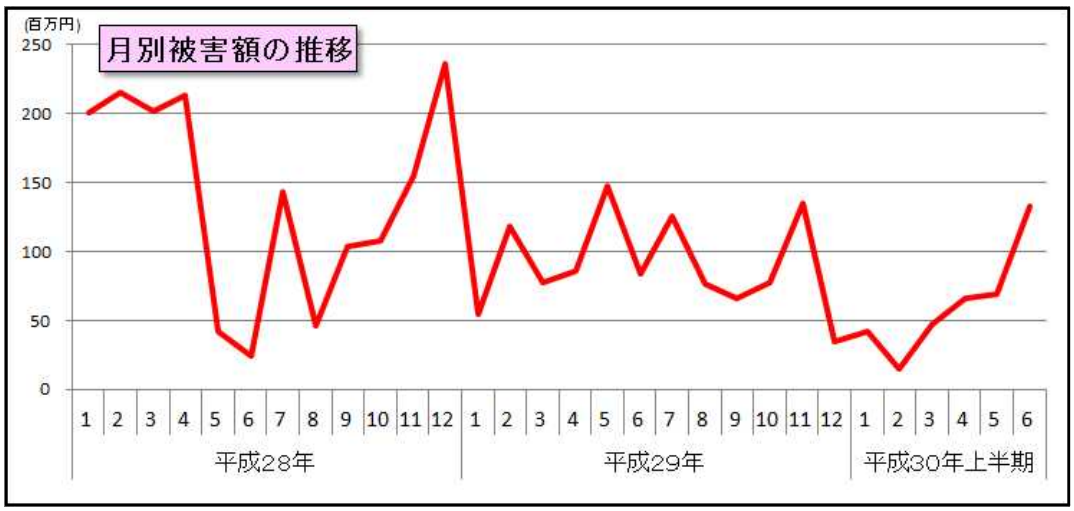
不正アクセス等、コンピュータ・ウイルスに関する相談

- 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。
- 仮想通貨交換業者が不正アクセスされ、仮想通貨をとられた。

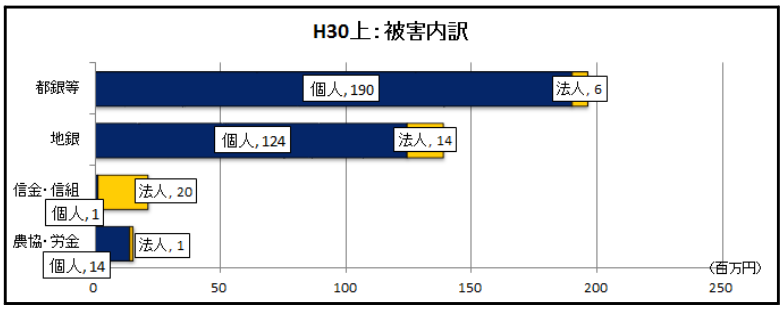
【　参考２　】

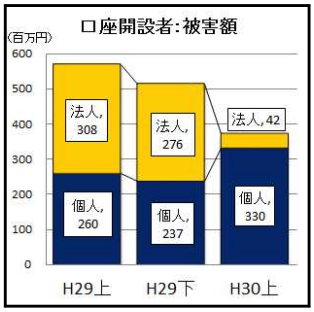
インターネットバンキングに係る不正送金事犯の発生状況

(1) 発生状況の推移



(2) 被害内訳

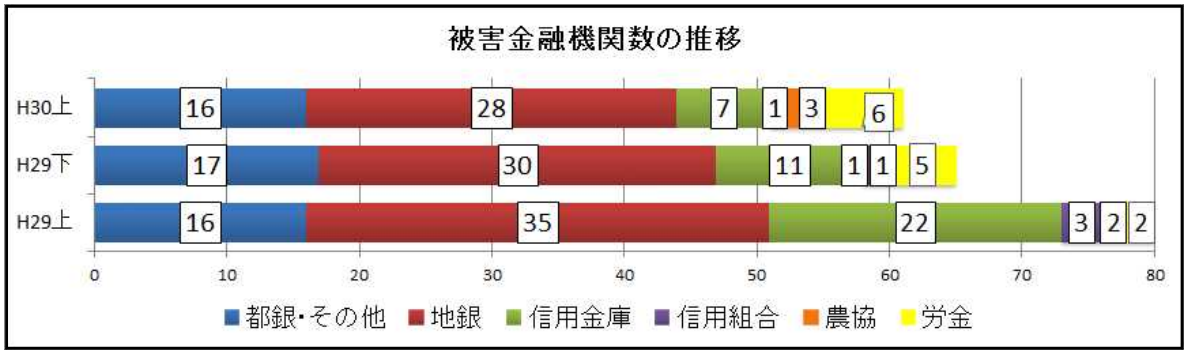




(3) 被害金融機関

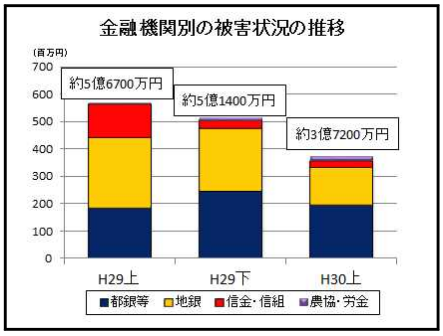
６１金融機関

都市銀行・信託銀行・ネット専業銀行・その他の銀行	１６行
地方銀行（第二地銀を含む。）	２８行
信用金庫	７金庫
信用組合	１組合
農業協同組合	３組合
労働金庫	６金庫



(4) 金融機関別の被害状況

金融機関別	H29上	H29下	H30上
都銀等	約1億8500万円	約2億4800万円	約1億9600万円
地　銀	約2億5900万円	約2億2700万円	約1億3900万円
信金・信組	約1億2000万円	約2900万円	約2100万円
農協・労金	約400万円	約900万円	約1600万円
合　計	約5億6700万円	約5億1400万円	約3億7200万円

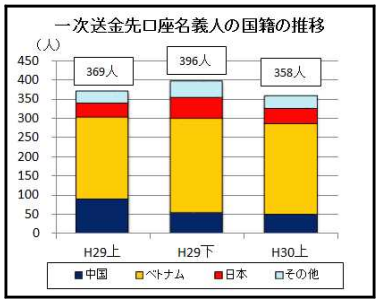


(5) 口座開設者別の被害状況

口座開設者		平成30年上半期				
		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1億9000万円 (51.1%)	約1億2400万円 (33.4%)	約100万円 (0.4%)	約1400万円 (3.8%)	約3億3000万円 (88.7%)
	実被害額	約1億7200万円 (51.4%)	約1億1200万円 (33.4%)	約100万円 (0.4%)	約1400万円 (4.2%)	約2億9900万円 (89.5%)
法人	被害額	約600万円 (1.7%)	約1400万円 (3.9%)	約2000万円 (5.3%)	約100万円 (0.4%)	約4200万円 (11.3%)
	実被害額	約300万円 (1.0%)	約1100万円 (3.4%)	約1900万円 (5.7%)	約100万円 (0.4%)	約3500万円 (10.5%)
合計	被害額	約1億9600万円 (52.8%)	約1億3900万円 (37.3%)	約2100万円 (5.7%)	約1600万円 (4.2%)	約3億7200万円 (100.0%)
	実被害額	約1億7500万円 (52.4%)	約1億2300万円 (36.8%)	約2000万円 (6.1%)	約1600万円 (4.6%)	約3億3400万円 (100.0%)

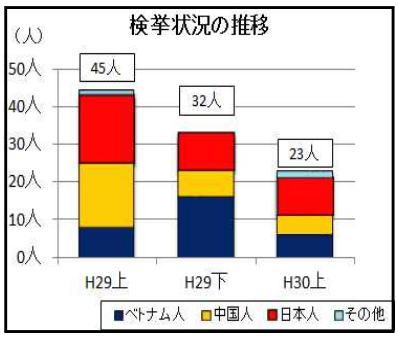
(6) 一次送金先口座名義人の国籍

	H29上		H29下		H30上	
中　国	93	25.2%	58	14.6%	52	14.5%
ベトナム	209	56.6%	243	61.4%	233	65.1%
日　本	37	10.0%	52	13.1%	41	11.5%
その他	30	8.1%	43	10.9%	32	8.9%
合　計	369	100.0%	396	100.0%	358	100.0%



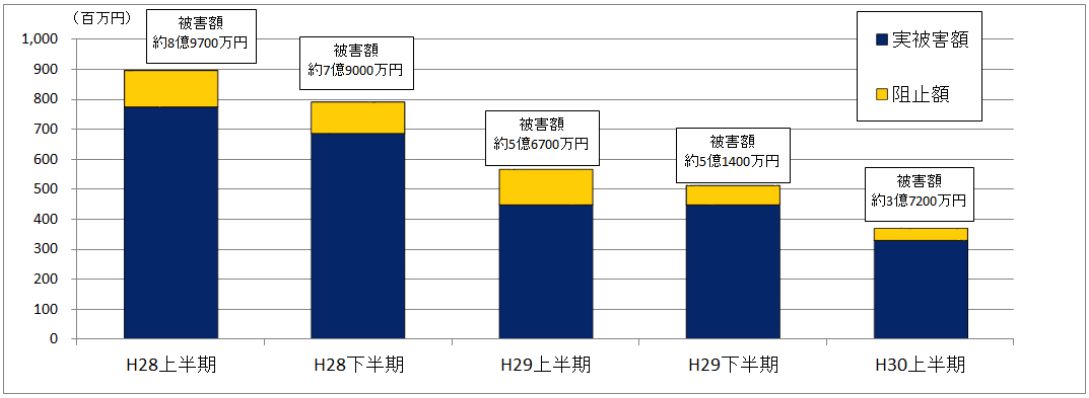
(7) 関連事件の検挙状況

		H29上		H29下		H30上	
検挙件数		28件		21件		18件	
検挙人数		45人		32人		23人	
内訳	中国人	17人	37.8%	7人	21.9%	5人	21.7%
	ベトナム人	8人	17.8%	16人	50.0%	6人	26.1%
	日本人	19人	42.2%	9人	28.1%	10人	43.5%
	その他	1人	2.2%	0人	0.0%	2人	8.7%



(8) 不正送金阻止状況

	被害額	実被害額	阻止額	阻止率
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4億4900万円	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%
H30上半期	約3億7200万円	約3億3400万円	約3800万円	10.2%



(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)	62	31.0%	122	61.0%	16	8.0%	200
電子証明書(法人口座)	3	27.3%	7	63.6%	1	9.1%	11