広　報　資　料
令和元年９月26日
警　　察　　庁

令和元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3,530.8件と増加傾向。

○　リモートデスクトップサービスを標的としたアクセスの急増を確認。

(2)　サイバー攻撃の情勢及び取組

○　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標的型メール攻撃を把握し、事業者に対して分析した情報を提供。

○　本年上半期に把握した標的型メール攻撃2,687件のうち、送信元メールアドレスが偽装されていると考えられるものが全体の90％を占め、引き続き高い割合。

○　本年上半期は、圧縮形式の添付ファイルのうち、実行ファイルが減少し、スクリプトファイルが増加。

２　サイバー犯罪の情勢等

(1)　サイバー犯罪の検挙状況

本年上半期の検挙件数は4,243件と、前年同期と同水準。

ア　不正アクセス禁止法違反

○　検挙件数は182件と、前年同期と同水準。

○　インターネットバンキングに係る不正送金事犯は、発生件数182件、被害額約１億6,500万円で、いずれも前年同期と比べて減少。

○　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は、認知件数９件、被害額約121万円相当で、いずれも前年同期と比べて大幅に減少。

イ　不正指令電磁的記録に関する罪及びコンピュータ・電磁的記録対象犯罪

○　検挙件数は175件と、前年同期と比べて増加。

(2)　主な取組

ＳＭＳを悪用し、通信事業者や運送系企業を装って、偽サイトに誘導するフィッシングの手口等について、日本サイバー犯罪対策センター（ＪＣ３）と連携して注意喚起を実施。

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

○　高度な実践型演習、検定及び学校教養を連携させた人材育成の推進

○　ＪＣ３等と連携した被害防止対策等の推進

○　2020年東京大会に向けたサイバーセキュリティ対策の推進

別　添

令和元年上半期におけるサイバー空間をめぐる脅威の情勢等

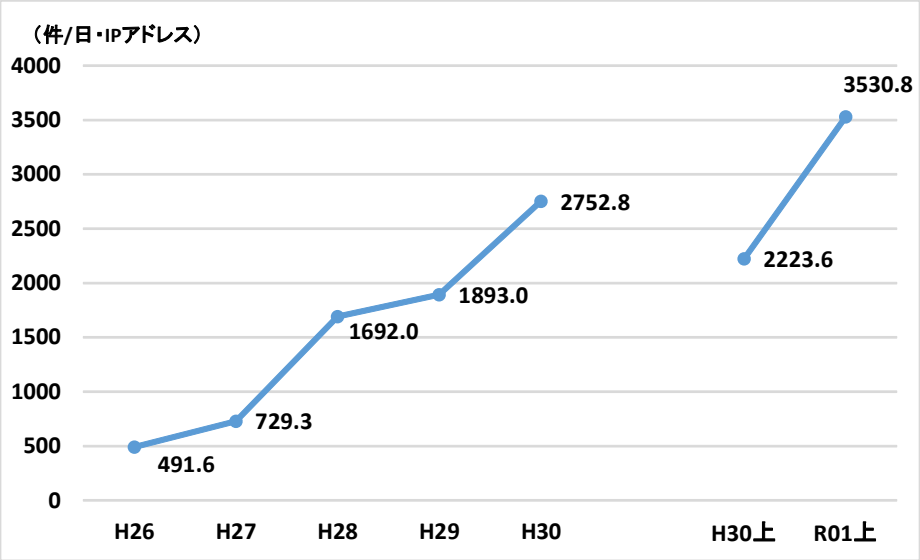
１　サイバー攻撃の情勢等

(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3,530.8件と、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

○　ＩｏＴ機器等のぜい弱性を狙ったアクセスの観測

本年６月中旬から、海外製デジタルビデオレコーダー等に使われる宛先ポート[*2] 5500/TCPや宛先ポート60001/TCPに対するMirai[*3] に感染したボットの特徴を有するアクセスが新たに観測されるようになった。当該ポートに対するアクセスには、外部サーバから不正プログラムのダウンロード及び実行を試みるものがあり、ＩｏＴ機器等のぜい弱性を悪用し、不正プログラムの感染拡大を狙ったものと考えられる。

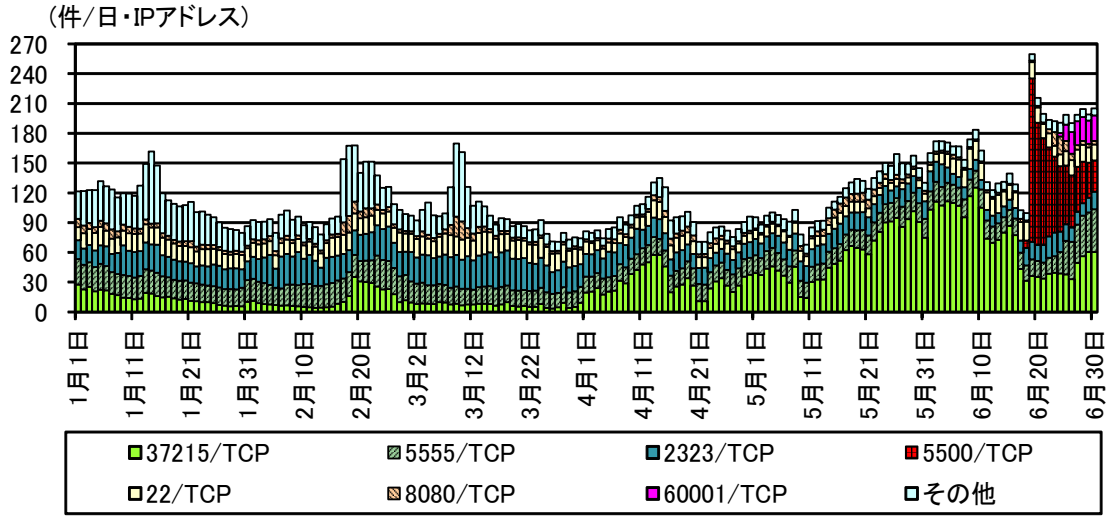
---

*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・UDP/IP通信において、通信を行うコンピュータが、利用するサービスを識別するためのインターフェースのこと。0から65535までの番号が割り当てられている。

*3　ＩｏＴ機器を感染対象とする不正プログラム

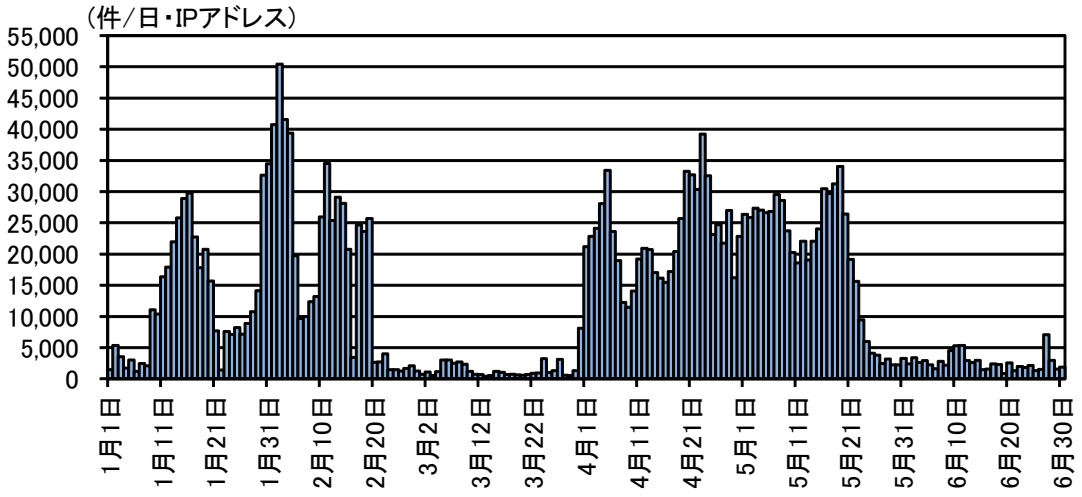
【図表２　Miraiボットの特徴を有するアクセス件数の推移（23/TCPを除く宛先ポート別）】



○　リモートデスクトップサービス[*4] を標的としたアクセスの増加

本年１月上旬から２月中旬までの間及び３月下旬から５月下旬までの間、Microsoft Windowsの遠隔操作に使用されるリモートデスクトップサービスを標的とした広範囲の宛先ポートに対するアクセスの急増を観測している。

【図表３　リモートデスクトップサービスを標的とした広範囲の宛先ポートに対するアクセス件数の推移】



当サービスについては、５月中旬、Microsoft社から、攻撃に成功すると外部から管理者権限で任意の操作が実行可能となるぜい弱性に関する緊急の修正プログラムが公開されている。

---

*4　職場等に設置されたコンピュータのデスクトップ環境を、別の場所に設置されたコンピュータ等から閲覧・操作などできるサービスであり、テレワーク等で利用されている。

(2)　サイバー攻撃の情勢及び取組

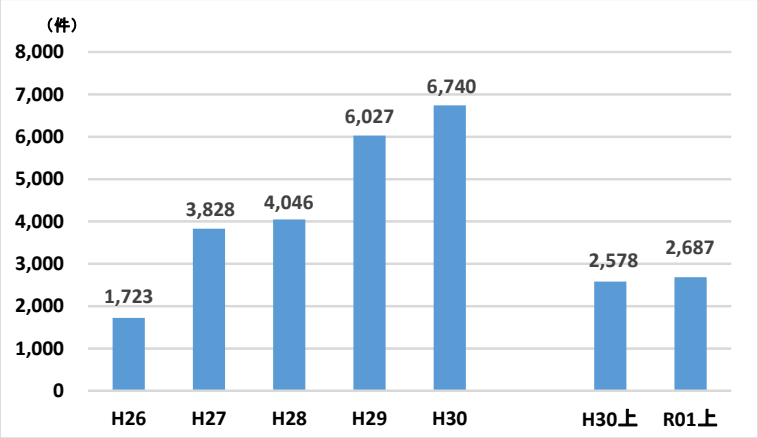
ア　情勢

(ｱ)　概況

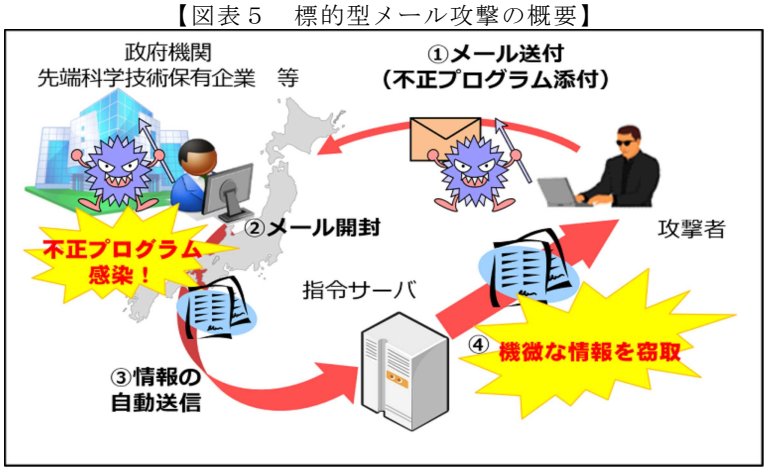
警察では、情報窃取を企図したとみられるサイバー攻撃に関する情報を、サイバーインテリジェンス情報共有ネットワーク[*5]により事業者等と共有し、集約された情報を総合的に分析し、事業者等に対し、分析結果に基づく情報提供を実施している。

本年上半期の同ネットワークを通じて把握した標的型メール攻撃[*6]の件数は2,687件と、前年同期と比べて増加した。

【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】



---

*5　警察と先端技術を有する全国約8,100の事業者等（令和元年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。

*6　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。

また、平成30年に引き続き、日本国内の公共交通機関、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。

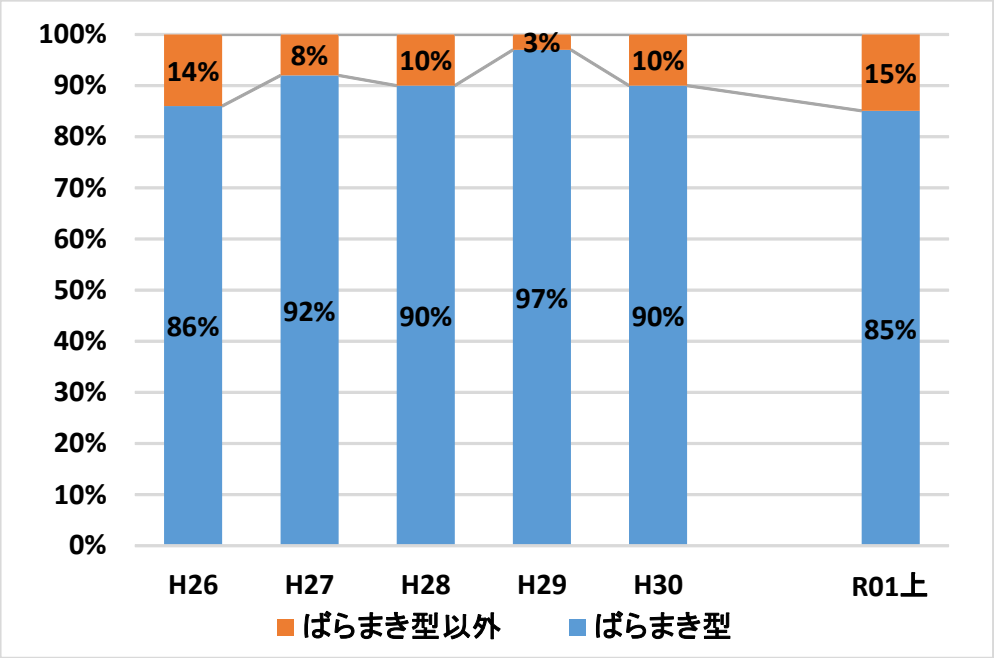
警察では、国際的ハッカー集団「アノニマス」を名乗る者が、日本国内の３組織に対してサイバー攻撃を実行したとする犯行声明とみられる投稿をＳＮＳ上に掲載している状況を把握している。

(ｲ)　標的型メール攻撃の手口等

○　「ばらまき型」攻撃[*7] の多発傾向が継続

「ばらまき型」攻撃が多数発生し、全体の85％を占め、引き続き高い割合となった。

【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の推移】



○　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82％を占めた。

○　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90％を占めた。

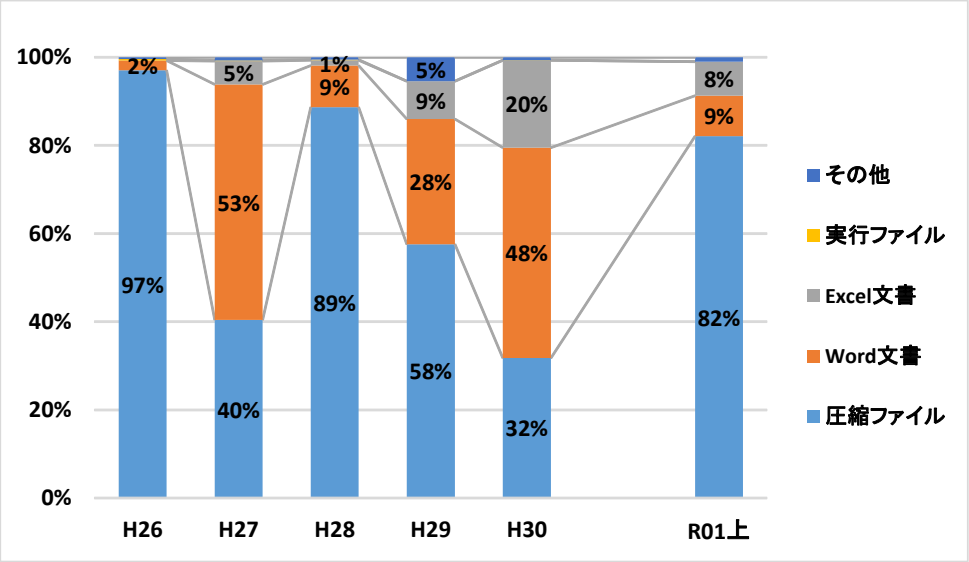
○　標的型メールに添付されたファイルの形式の変化

標的型メールに添付されたファイルの形式については、本年上半期は、前年約７割を占めたWord形式、Excel形式のファイルの割合が減少し、圧縮ファイルの割合が増加した。

---

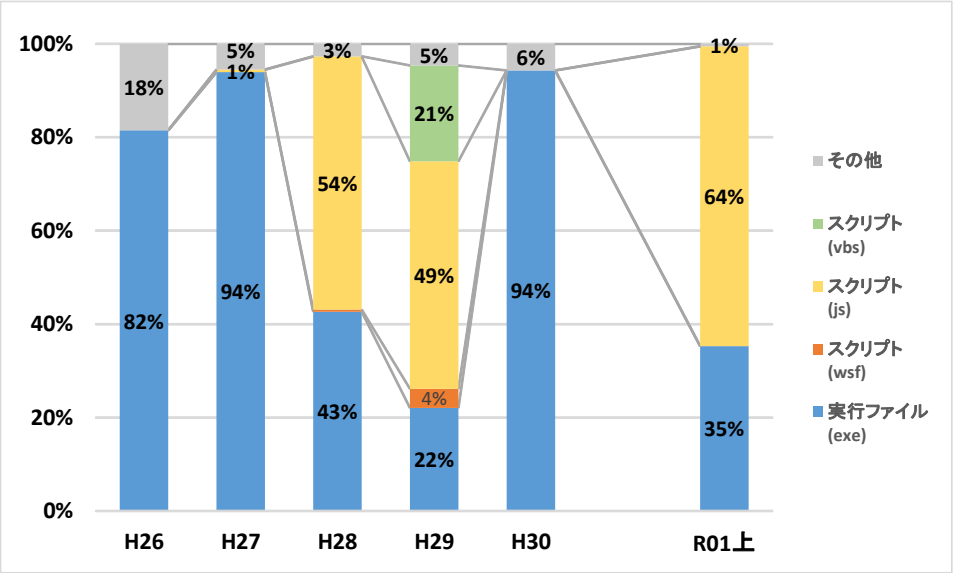
*7　標的型メール攻撃のうち、同じ文面や不正プログラムが10か所以上に送付されていたものを「ばらまき型」として集計している。

【図表７　標的型メールに添付されたファイルの形式の割合の推移】



圧縮ファイルで送付されたファイルの形式については、平成28年及び29年に半数以上を占めていたスクリプトファイル[*8]が再び高い割合を示した。

【図表８　圧縮ファイルで送付されたファイル形式の割合の推移】



標的型メール攻撃の手法は日々変化しているとみられるため、引き続きその動向を注視しながら対策を講じる必要がある。

○　事例

・　注文内容の確認と称し、添付ファイルを開くよう誘導するメール

*8　簡易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。

が、事業者の非公開メールアドレスに対して送信された。

・　国際情勢に関する資料の送付と称して、添付された圧縮ファイルを解凍し、生成されたファイルを開くよう誘導するメールが、送信元メールアドレスを偽装して事業者に対して送信された。

イ　取組

(ｱ)　サイバーテロ対策協議会

各都道府県警察と重要インフラ事業者等により構成されるサイバーテロ対策協議会の枠組み等を通じ、個別訪問によるサイバー攻撃の脅威や情報セキュリティに関する情報提供等を行っている。また、サイバー攻撃の発生を想定した共同対処訓練を実施するなど、緊急対処能力の向上に努めている。

(ｲ)　サイバー攻撃事案で使用されたＣ２サーバ[*9] 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、本年上半期においては１台の機能停止が実施された。

(ｳ)　2020年東京大会に向けたサイバー攻撃対策の推進

2020年東京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、外国の関係機関等との情報交換等の取組を推進した。

---

*9　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。

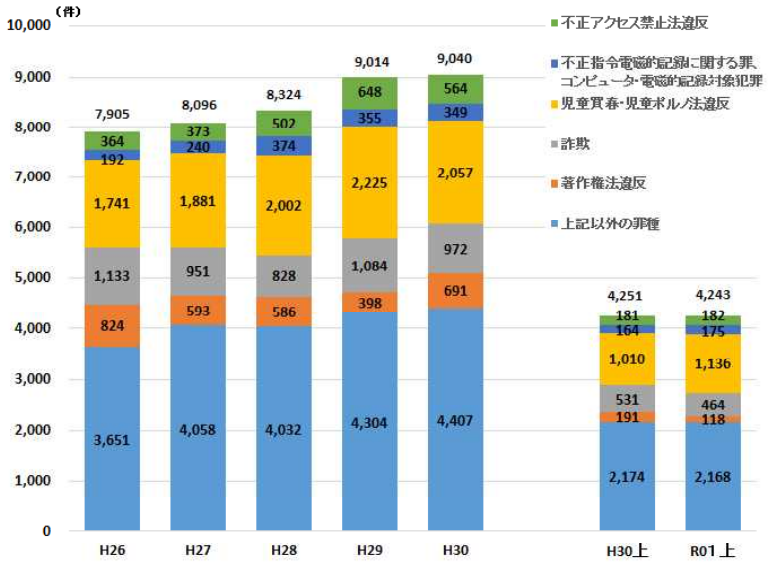
2　サイバー犯罪の情勢等

(1)　サイバー犯罪の検挙状況

ア　サイバー犯罪の検挙件数

サイバー犯罪の検挙件数は増加傾向にあり、本年上半期の検挙件数は4,243件と、前年同期と同水準となった。

【図表９　サイバー犯罪の検挙件数の推移】

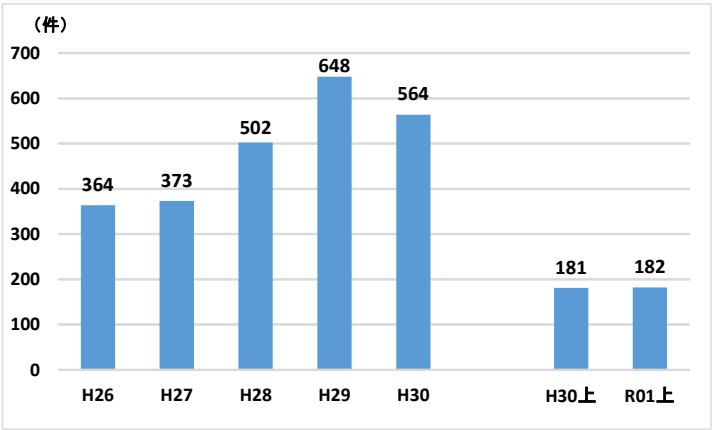


イ　不正アクセス禁止法[*10]　違反

(ｱ)　検挙件数等

○　本年上半期における不正アクセス禁止法違反の検挙件数は182件と、前年同期と同水準となった。検挙件数のうち、159件が識別符号窃用型[*11]で全体の約87.4％を占めている。

【図表10　不正アクセス禁止法違反の検挙件数の推移】



---

*10　不正アクセス行為の禁止等に関する法律（「不正アクセス行為・他人の識別符号を不正に取得する行為・不正アクセス行為を助長する行為・他人の識別符号を不正に保管する行為・識別符号の入力を不正に要求する行為」の５つの違反行為が定められている。）

*11　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

○　「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」が最多

識別符号窃用型の不正アクセス行為に係る手口では、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37件と最も多く、全体の約23.3%を占めており、次いで他人から入手したものが28件で全体の約17.6%となっている。

○　被疑者が不正に利用したサービスは「社員・会員用等の専用サイト」が最多

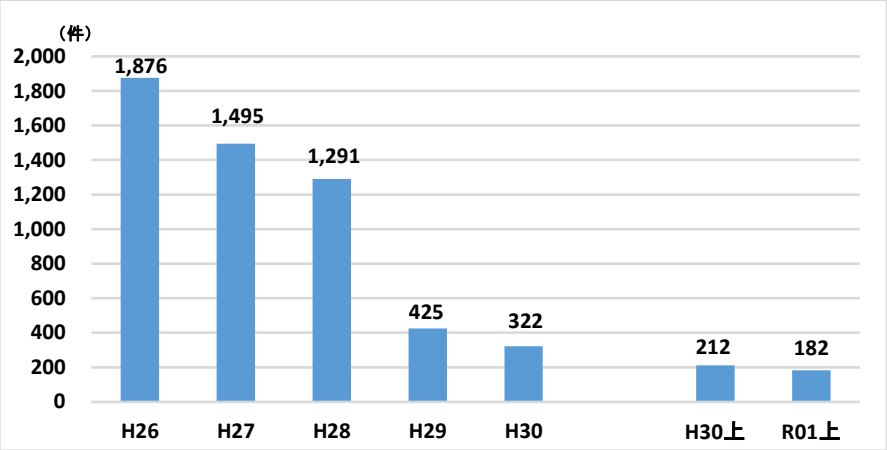
被疑者が不正に利用したサービスは、社員・会員用等の専用サイトが37件と最も多く、全体の約23.3%を占めており、次いでオンラインゲーム・コミュニティサイトが34件で全体の約21.4%を占めている。

(ｲ)　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

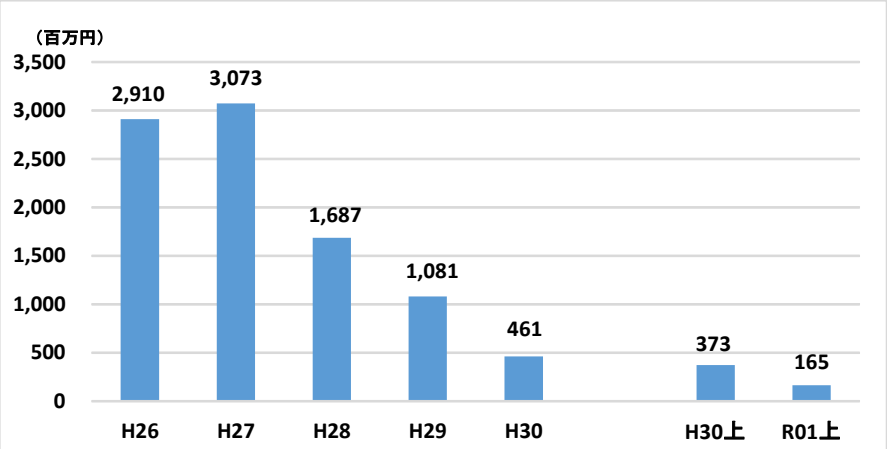
○　概況

本年上半期における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182件、被害額約１億6,500万円で、いずれも前年同期と比べて減少した。

【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】



○　特徴

モニタリング[*12] の強化、ワンタイムパスワードの導入等の対策により、平成28年以降、発生件数・被害額はともに減少傾向が続いている。

一次送金先として把握した194口座のうち、名義人の国籍はベトナムが約44.3％を占め、次いで日本が約15.5％、中国が約11.9％であった。

(ｳ)　仮想通貨[*13] 交換業者等への不正アクセス等による不正送信事犯

本年上半期における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については、認知件数９件、被害額約121万円相当で、いずれも前年同期（認知件数158件、被害額約605億300万円相当）と比べて大幅に減少した。

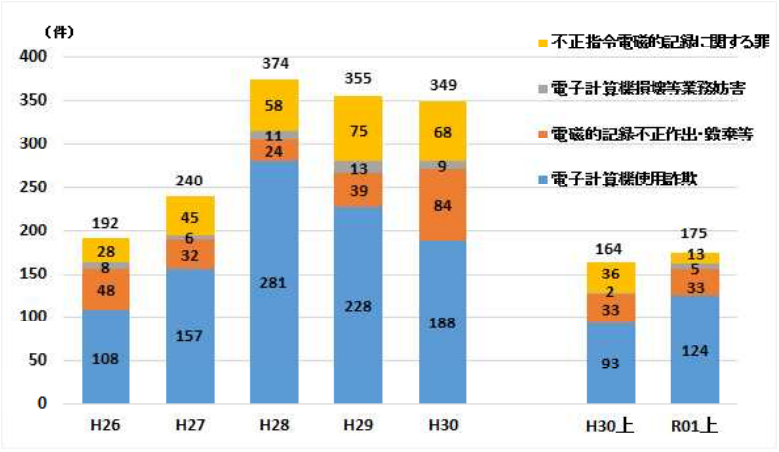
仮想通貨交換業者等において対策が講じられている一方で、本年７月には、国内の仮想通貨交換業者から約30億円相当の仮想通貨が不正に送信されたとみられる事案が発生しており、予断を許さない状況にある。

ウ　不正指令電磁的記録に関する罪[*14] 及びコンピュータ・電磁的記録対象犯罪[*15]

○　検挙件数

本年上半期における不正指令電磁的記録に関する罪及びコンピュータ・電磁的記録対象犯罪の検挙件数は175件で、前年同期と比べて増加した。

【図表13　不正指令電磁的記録に関する罪及びコンピュータ・電磁的記録対象犯罪の検挙件数の推移】



---

*12　不正送金に使用されたＩＰアドレス等に対する監視

*13　令和元年（2019年）、第198回国会において、「仮想通貨」の呼称の「暗号資産」への変更等を内容とする情報通信技術の進展に伴う金融取引の多様化に対応するための資金決済に関する法律等の一部を改正する法律が成立した。

*14　刑法第168条の２第１項（不正指令電磁的記録作成、提供）、同法第168条の２第２項（不正指令電磁的記録供用）、同法第168条の３（不正指令電磁的記録取得、保管）

*15　刑法第161条の２第１項（私電磁的記録不正作出）、同法第161条の２第２項（公電磁的記録不正作出）、同法第163条の２第１項（支払用カード電磁的記録不正作出）、同法第234条の２（電子計算機損壊等業務妨害（電子計算機を物理的に損壊し業務を妨害した事犯を除く））、同法第246条の２（電子計算機使用詐欺）、同法第258条（公用電磁的記録毀棄）、同法第259条（私用電磁的記録毀棄）

○　特徴

検挙件数のうち、電子計算機使用詐欺が124件と最も多く、全体の約70.9％を占めている。

エ　その他

○　児童買春・児童ポルノ法違反の検挙件数は1,136件で、前年同期と比べて増加した。

○　著作権法違反の検挙件数は118件で、前年同期と比べて減少した。

(2)　取組

○　インターネットバンキングに係る不正送金事犯の被害防止対策

インターネットバンキングを利用して、プリペイドカードを繰り返し大量に購入する手口の不正送金事犯の発生を受け、事業者に対して、モニタリングの強化、１日当たりの購入回数制限の設定等を働き掛けた。

○　ＳＭＳを悪用したフィッシング等に係る対策

ＳＭＳの送信元を偽装し、正規の通信事業者と同一スレッド内にメッセージとＵＲＬを挿入して偽サイトに誘導するフィッシングの手口や、運送系企業を装ったＳＭＳに記載したＵＲＬから偽サイトに誘導して携帯電話番号及びＳＭＳ認証コードを不正取得し、キャッシュレス決済のアカウントを作成する手口等について、ＪＣ３と連携し、ＳＭＳで受信したＵＲＬが正規事業者のＵＲＬかどうかを確認することなどの被害防止に関する注意喚起を実施した。

○　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

愛知県警察とＪＣ３が共同で開発したツールの活用等により、ＪＣ３が発見した詐欺サイトのＵＲＬ情報をＡＰＷＧ[*16] 等に提供し、被害防止対策を実施している。

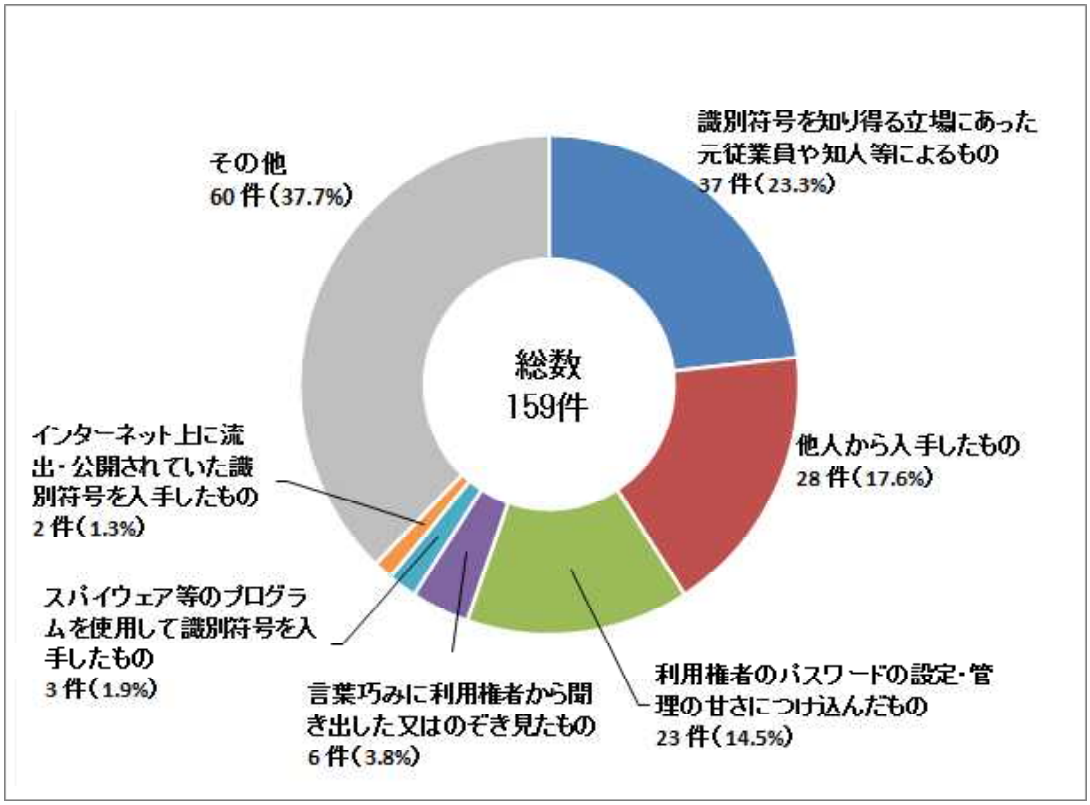
---

*16　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。

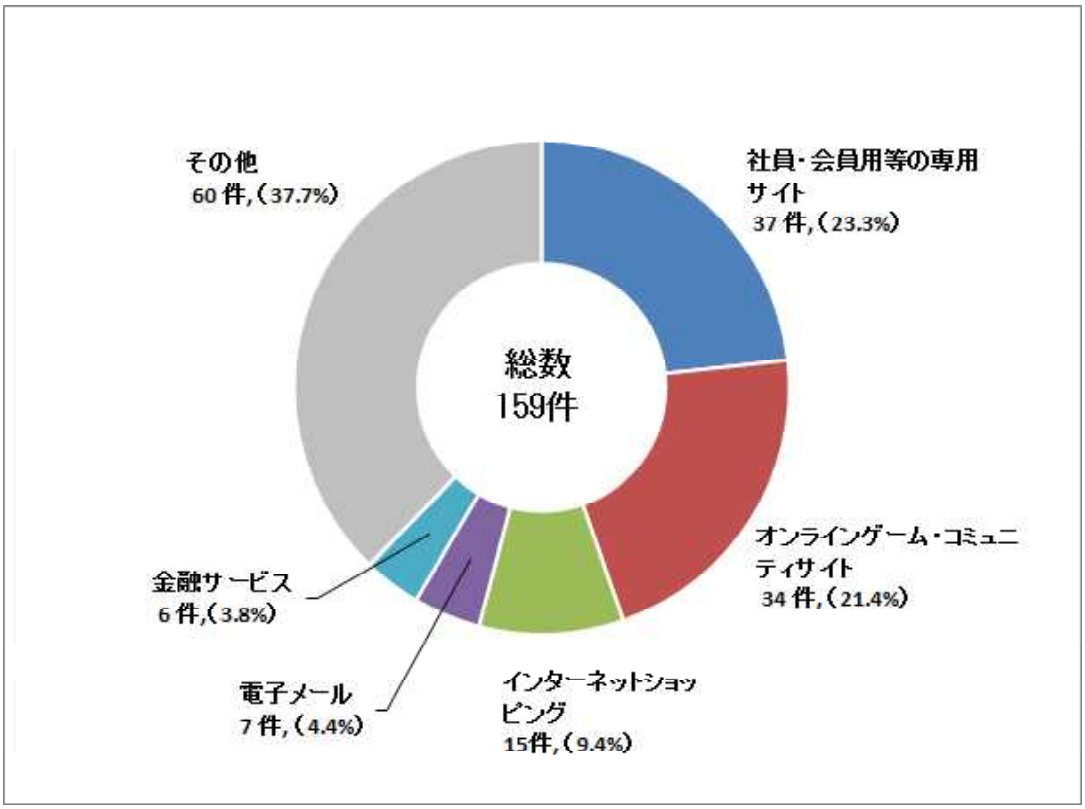
【　参考　】

1　不正アクセス禁止法違反の検挙状況等

(1) 不正アクセス行為（識別符号窃用型）に係る手口別検挙件数



(2) 不正に利用されたサービス別検挙件数（識別符号窃用型）



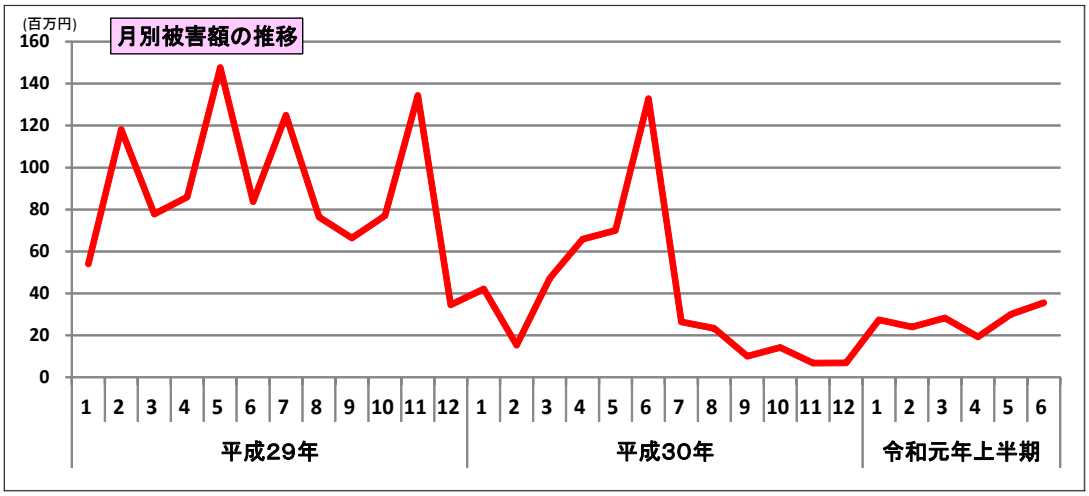
不正アクセス禁止法違反

○　無職の男（62）は、平成30年11月、インターネットサービスプロバイダの会員サイトに対して、他人のＩＤ・パスワードを使用して不正アクセスし、パスワード等を変更した。平成31年２月、男を不正アクセス禁止法違反（不正アクセス行為）等で検挙した。（栃木）

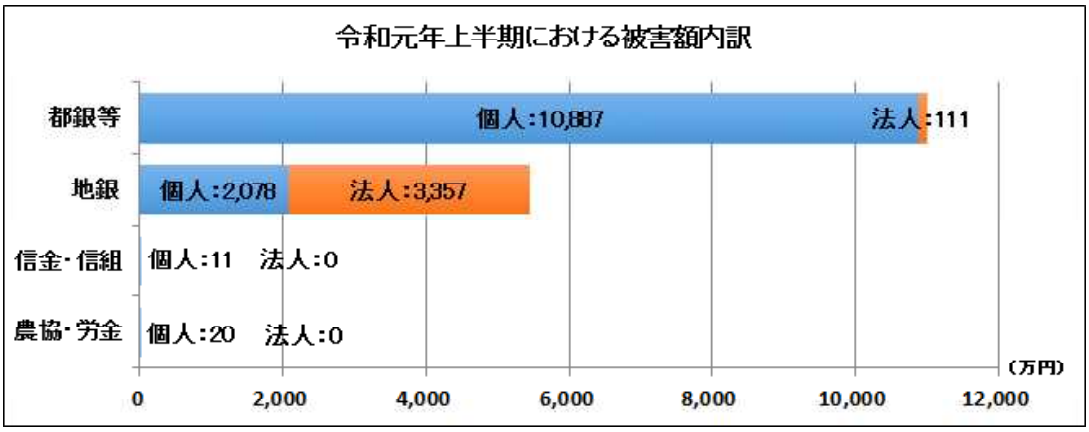
○　無職の男（27）は、平成30年９月、大手企業の会員サイトに対して、他人のＩＤ・パスワードを使用して不正アクセスし、ポイントを自らが作成したアカウントに移動した。平成31年３月、男を不正アクセス禁止法違反（不正アクセス行為）等で検挙した。（千葉）

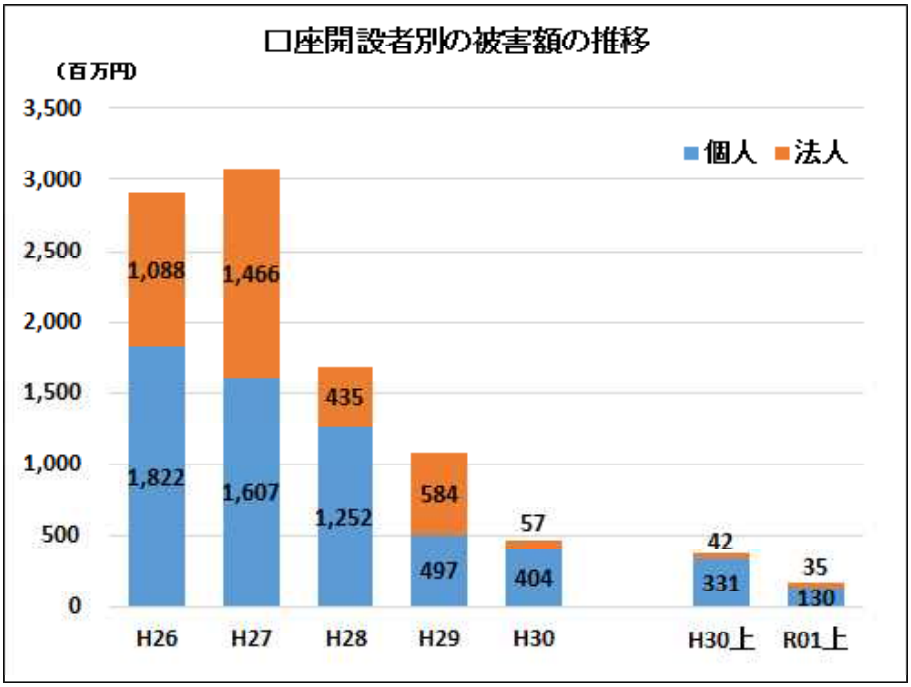
2　インターネットバンキングに係る不正送金事犯の発生状況等

(1) 発生状況の推移

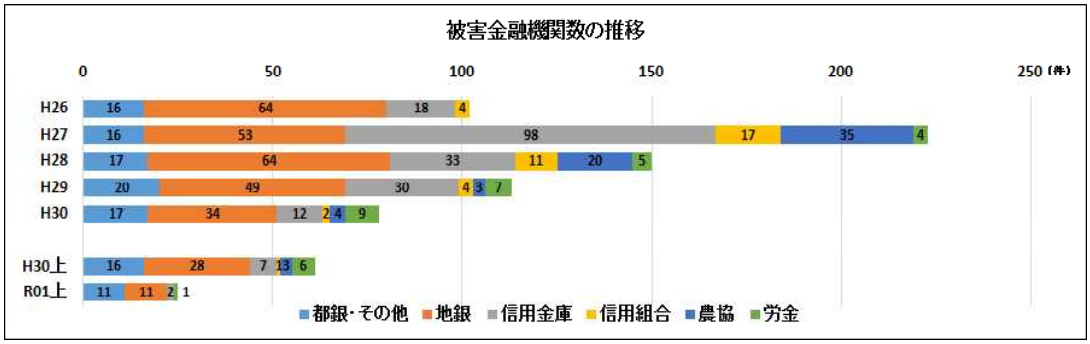


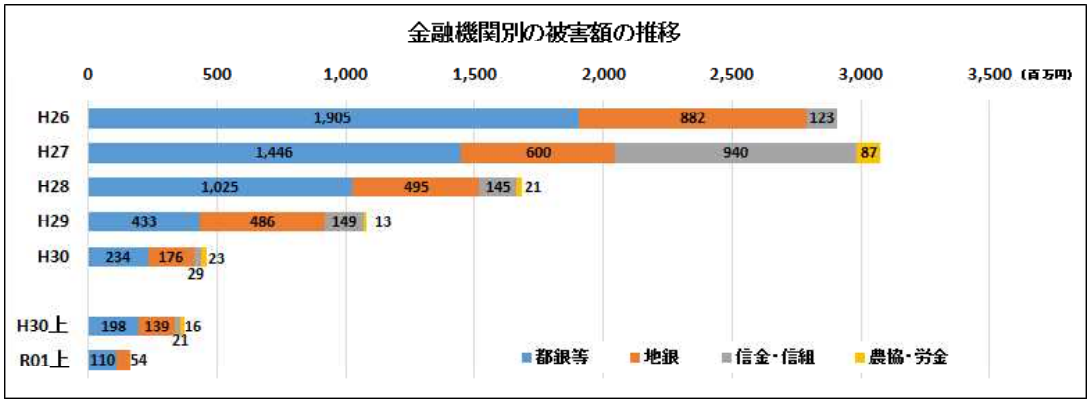
(2) 被害額内訳





(3) 金融機関別の被害状況

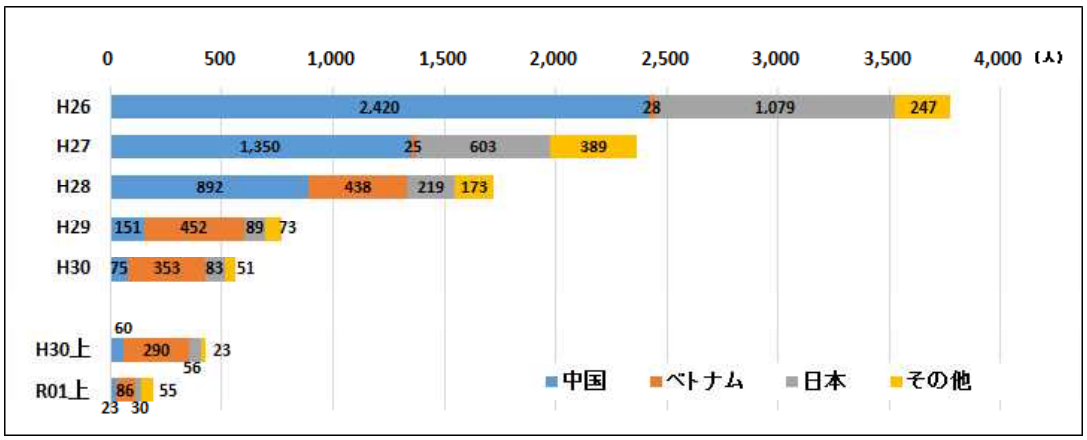




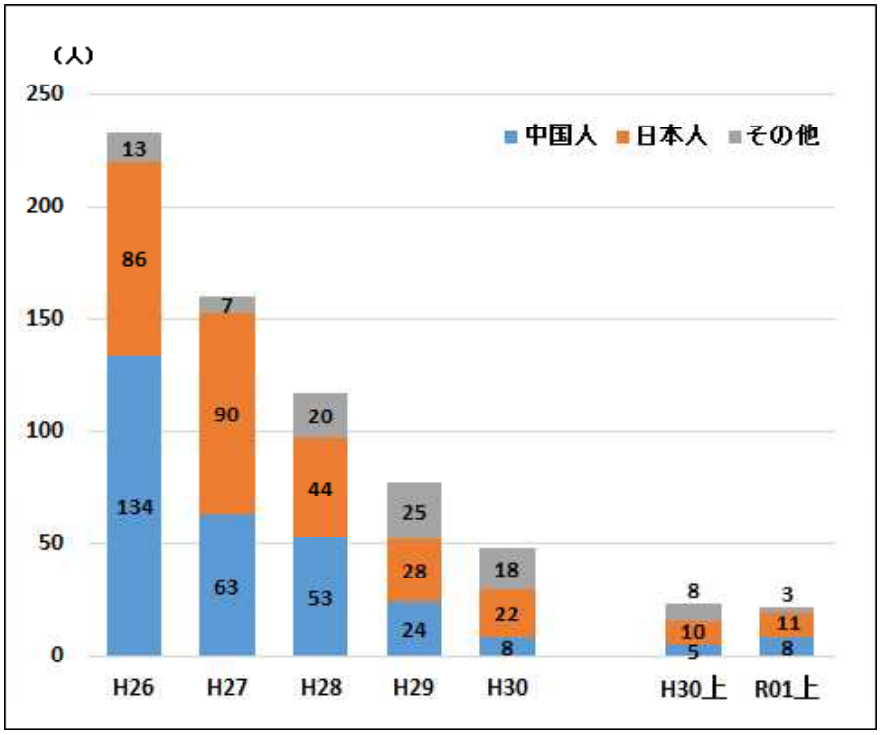
(4) 口座開設者別の被害状況

口座開設者		令和元年上半期				
		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1億887万円 (66.1%)	約2,078万円 (12.6%)	約11万円 (0.1%)	約20万円 (0.1%)	約1億2,996万円 (78.9%)
	実被害額	約8,973万円 (61.7%)	約2,078万円 (14.3%)	約11万円 (0.1%)	約20万円 (0.1%)	約1億1,082万円 (76.2%)
法人	被害額	約111万円 (0.7%)	約3,357万円 (20.4%)	0円 (0.0%)	0円 (0.0%)	約3,468万円 (21.1%)
	実被害額	約111万円 (0.8%)	約3,357万円 (23.1%)	0円 (0.0%)	0円 (0.0%)	約3,468万円 (23.8%)
合計	被害額	約1億998万円 (66.8%)	約5,435万円 (33.0%)	約11万円 (0.1%)	約20万円 (0.1%)	約1億6,464万円 (100.0%)
	実被害額	約9,084万円 (62.4%)	約5,435万円 (37.4%)	約11万円 (0.1%)	約20万円 (0.1%)	約1億4,551万円 (100.0%)

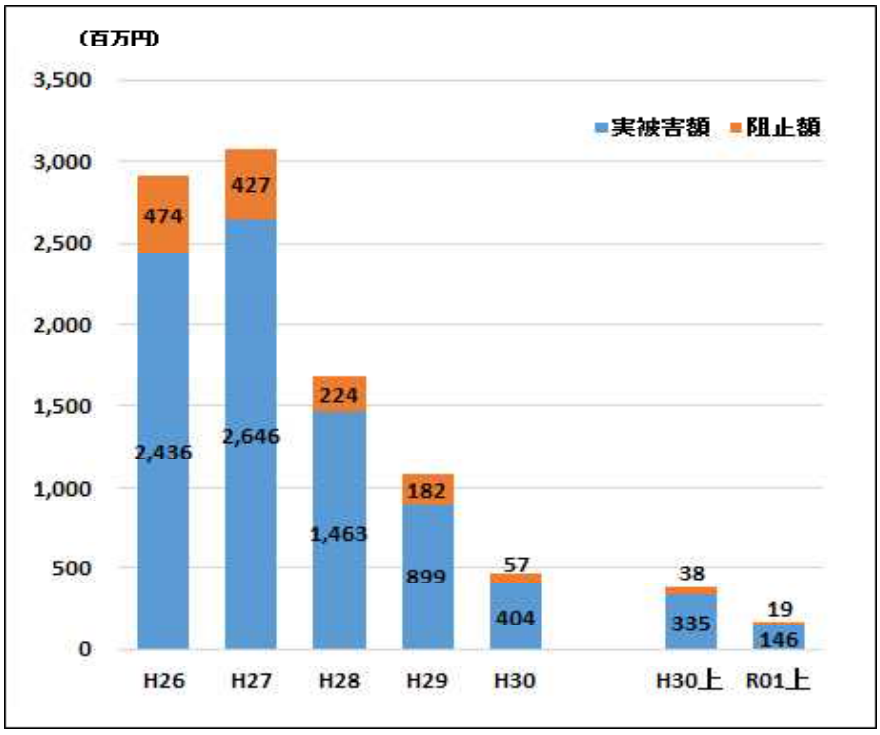
(5) 一次送金先口座名義人の国籍



(6) 国籍別の関連事件検挙状況



(7) 不正送金阻止状況



(8) 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）	118	68.6%	49	28.5%	5	2.9%	172
電子証明書（法人口座）	4	40.0%	6	60.0%	0	0.0%	10

３　不正指令電磁的記録に関する罪及びコンピュータ・電磁的記録対象犯罪の検挙状況

(1) 検挙件数の推移

	H26	H27	H28	H29	H30	H30(上)	R1(上)
電子計算機使用詐欺	108	157	281	228	188	93	124
電磁的記録不正作出・毀棄等	48	32	24	39	84	33	33
電子計算機損壊等業務妨害	8	6	11	13	9	2	5
不正指令電磁的記録供用	16	21	36	24	37	16	6
不正指令電磁的記録取得・保管	3	16	18	22	19	14	4
不正指令電磁的記録作成・提供	9	8	4	29	12	6	3

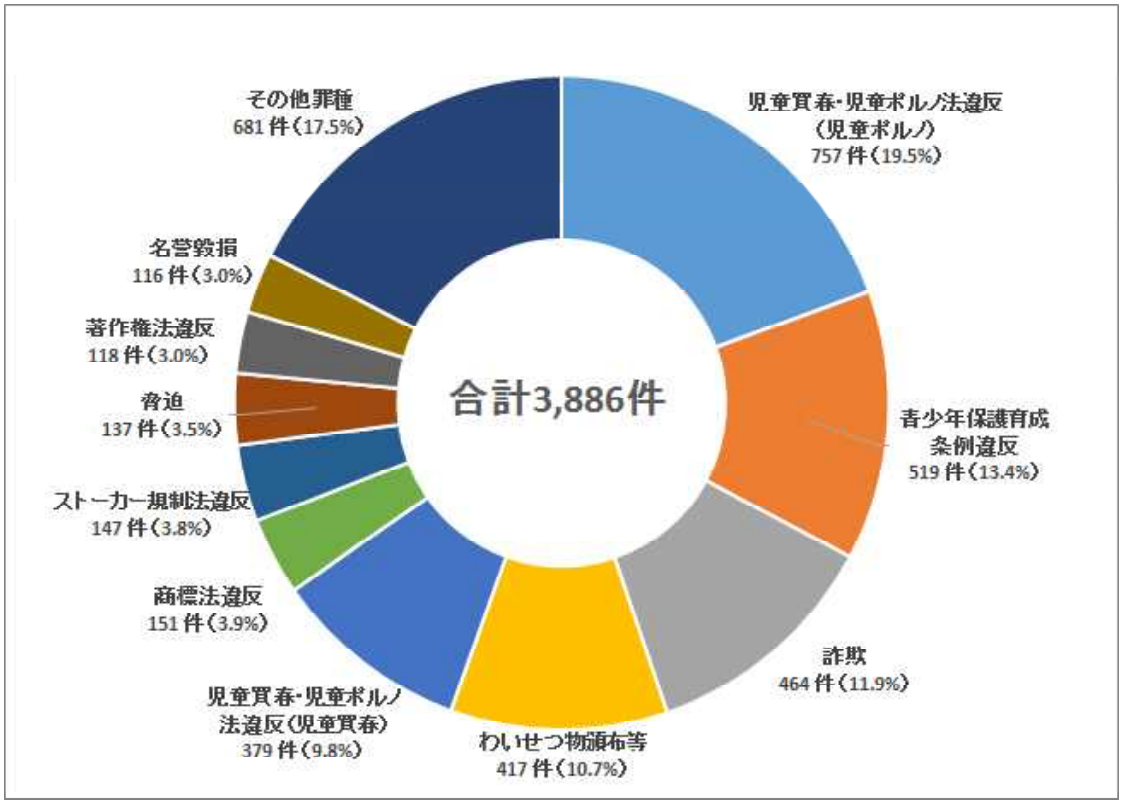
コンピュータ・電磁的記録対象犯罪

○　専門学校生の少年（18）は、平成30年８月から９月までの間、仮想通貨関連サービスに使用するサーバコンピュータに虚偽の情報を与え、同サービスの運営会社が管理する仮想通貨（暗号資産）合計約1,500万円相当を移転させた。平成31年３月、少年を電子計算機使用詐欺罪等で検挙した。（警視庁）

不正指令電磁的記録に関する罪

○　無職の男（54）は、平成29年３月、サイト閲覧者のパソコンに不当な料金請求画面を繰り返し表示させる不正プログラムを供用し、真正なものと誤信させ現金を詐取した。令和元年５月、男を不正指令電磁的記録供用罪・詐欺罪で検挙した。（宮城、茨城、静岡、石川、愛知、愛媛、鹿児島）

４　その他



詐欺

○　会社役員の男（36）らは、平成30年２月から同年10月までの間、フィッシングサイトによって不正に入手した他人のメールアカウントを使用し、虚偽の儲け話を持ち掛け、電子マネーを詐取した。令和元年６月、男らを詐欺で検挙した。（埼玉）

電気通信事業法違反

○　自営業の女（27）は、平成30年２月頃から同年６月頃までの間、総務大臣に届出をしないで、国内外の利用者からの接続を中継する機能を有する中継サーバコンピュータを保守管理し、無届で電気通信事業を営んだ。令和元年５月、女を電気通信事業法違反で検挙した。（茨城）