不正アクセス行為の発生状況

第１　平成30年における不正アクセス禁止法違反事件の認知・検挙状況等について

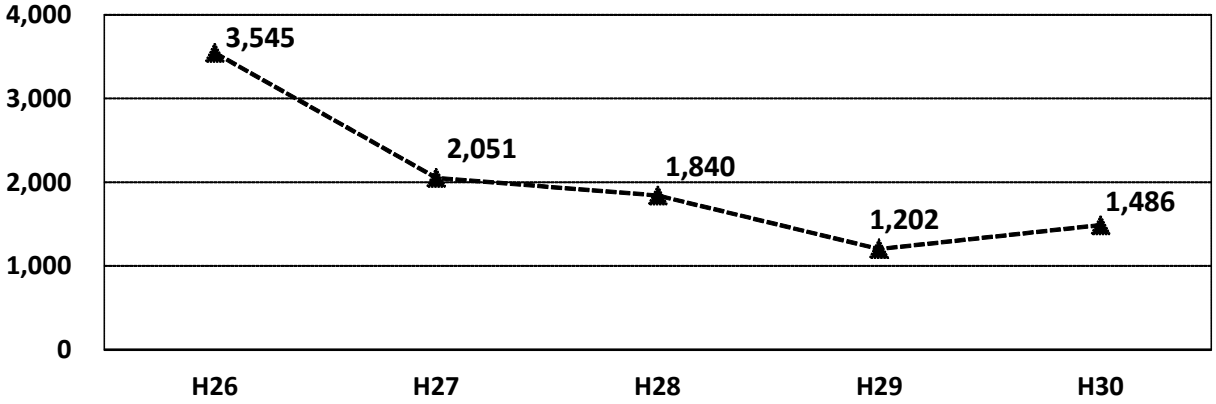
平成30年に都道府県警察から警察庁に報告のあった不正アクセス行為を対象とした。

１　不正アクセス行為の認知状況

(1)　認知件数

平成30年における不正アクセス行為の認知件数[注1]は1,486件であり、平成26年と比較して約58.1%減少したものの、前年から284件増加した。

（件）　図１－１　過去５年の不正アクセス行為の認知件数の推移



(2)　不正アクセスを受けた特定電子計算機のアクセス管理者

不正アクセス行為の認知件数について、不正アクセスを受けた特定電子計算機のアクセス管理者[注2]別に内訳を見ると、「一般企業」が最も多く1,314件となっている。

表１－１　過去５年の不正アクセスを受けた特定電子計算機のアクセス管理者別認知件数

区分＼年次	平成26年	平成27年	平成28年	平成29年	平成30年
一般企業	3,468	1,998	1,823	1,177	1,314
大学、研究機関等	56	11	2	5	161
行政機関等	3	14	5	9	6
プロバイダ	16	11	6	6	4
その他	2	17	4	5	1
計(件)	3,545	2,051	1,840	1,202	1,486

※「大学、研究機関等」には、高等学校等の教育機関を含む。
※「行政機関等」には、独立行政法人、特殊法人、地方公共団体及びこれらの附属機関を含む。
※「プロバイダ」とは、インターネットに接続する機能を提供する電気通信事業者をいう。

注1　ここでいう認知件数とは、不正アクセス被害の届出を受理した場合のほか、余罪として新たな不正アクセス行為の事実を確認した場合、報道を踏まえて事業者等に不正アクセス行為の事実を確認した場合その他関係資料により不正アクセス行為の事実を確認することができた場合において、被疑者が行った犯罪構成要件に該当する行為の数をいう。

注2　特定電子計算機とは、ネットワークに接続されたコンピュータをいい、アクセス管理者とは、特定電子計算機を誰に利用させるかを決定する者をいう。

(3)　認知の端緒

不正アクセス行為の認知件数について、認知の端緒別に内訳を見ると、「利用権者[注3]からの届出によるもの」が最も多く（852件）、次いで「不正アクセスを受けた特定電子計算機のアクセス管理者からの届出によるもの」（345件）、「警察職員による特定電子計算機のアクセスログ解析等の警察活動によるもの」（269件）の順となっている。

図１－２　平成30年における認知の端緒別認知件数

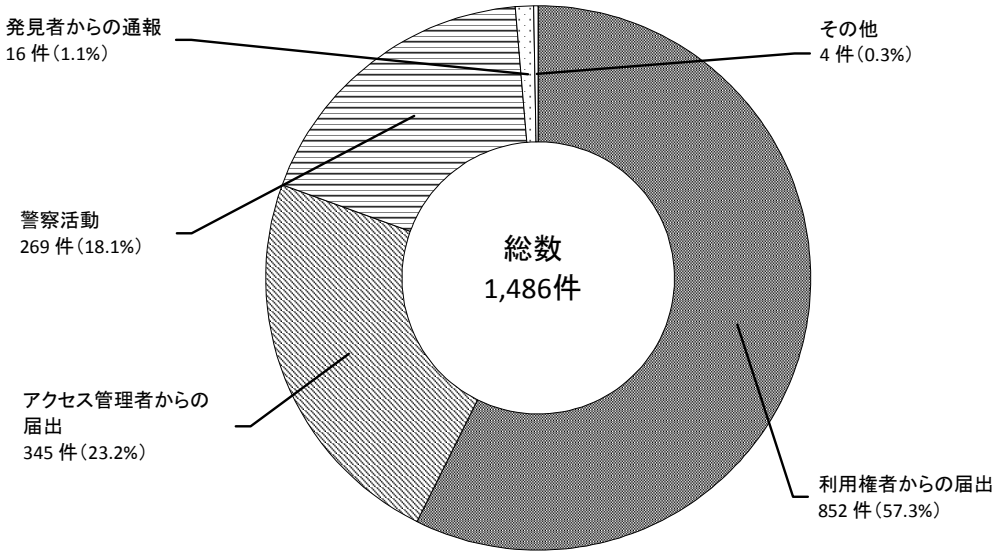


表１－２　過去５年の認知の端緒別認知件数

区分＼年次	平成26年	平成27年	平成28年	平成29年	平成30年
利用権者からの届出	1,337	614	495	655	852
アクセス管理者からの届出	1,848	910	828	255	345
警察活動	119	516	511	283	269
発見者からの通報	238	11	5	6	16
その他	3	0	1	3	4
計（件）	3,545	2,051	1,840	1,202	1,486

注3　利用権者とは、ネットワークを通じて特定電子計算機を利用することについて、当該特定電子計算機のアクセス管理者の許諾を得た者をいう。例えば、プロバイダからインターネット接続サービスを受けることを認められた会員や企業からＬＡＮを利用することを認められた社員が該当する。

(4)　不正アクセス後の行為

不正アクセス行為の認知件数について、不正アクセス後に行われた行為別に内訳を見ると、「メールの盗み見等の情報の不正入手」が前年から約2.6倍に増加して最も多く（385件）、次いで「インターネットバンキングでの不正送金等」（330件）、「オンラインゲーム・コミュニティサイトの不正操作」（199件）の順となっている。

図１－３　平成30年における不正アクセス後の行為別認知件数

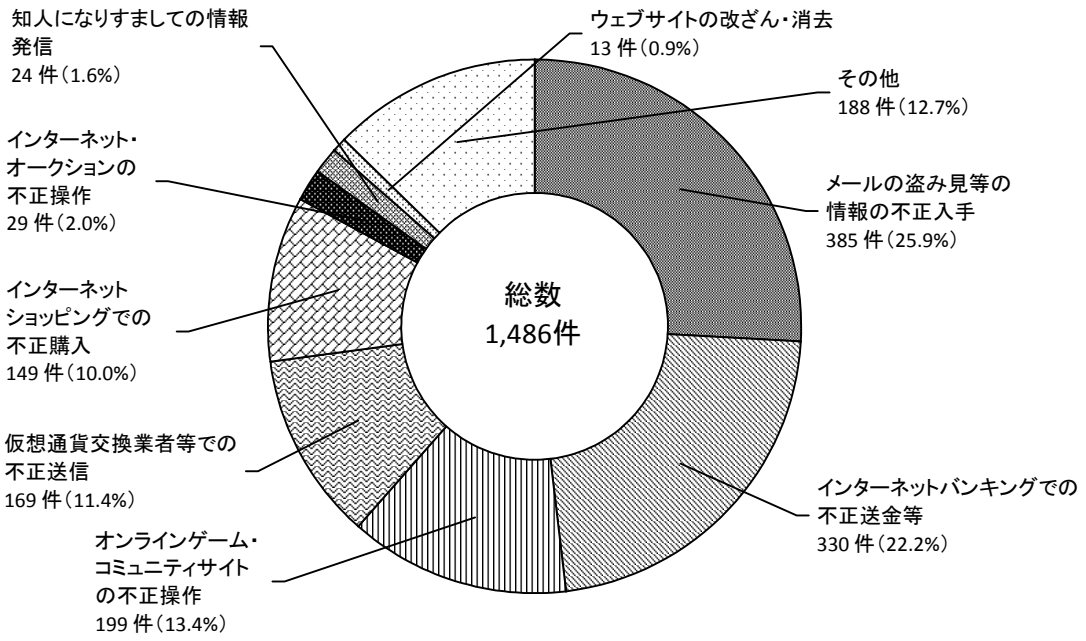


表１－３　過去５年の不正アクセス後の行為別認知件数

区分＼年次	平成26年	平成27年	平成28年	平成29年	平成30年
メールの盗み見等の情報の不正入手	177	92	91	146	385
インターネットバンキングでの不正送金等	1,944	1,531	1,305	442	330
オンラインゲーム・コミュニティサイトの不正操作	130	96	124	83	199
仮想通貨交換業者等での不正送信				149	169
インターネットショッピングでの不正購入	209	167	172	133	149
インターネット・オークションの不正操作	13	20	34	28	29
知人になりすましての情報発信	1,009	83	25	110	24
ウェブサイトの改ざん・消去	40	34	6	14	13
その他	23	28	83	97	188
計（件）	3,545	2,051	1,840	1,202	1,486

※　平成28年以前は、「仮想通貨交換業者等での不正送信」を分類して集計していない。

2　不正アクセス禁止法違反事件の検挙状況

(1)　検挙件数等

平成30年における不正アクセス禁止法違反の検挙件数は564件、検挙人員は173人であり、前年と比べ、検挙件数は84件、検挙人員は82人いずれも減少した。

検挙件数及び検挙人員について違反行為別に内訳を見ると、「不正アクセス行為」が520件、164人といずれも約９割を占めており、他の類型については「識別符号の提供（助長）行為[注4]」が４件、４人、「識別符号の取得行為[注5]」が22件、２人、「識別符号の保管行為[注6]」が16件、12人、「フィッシング行為[注7]」が２件、２人であった。

表２－１　過去５年の違反行為別検挙件数等

区分＼年次		平成26年	平成27年	平成28年	平成29年	平成30年
不正アクセス行為	検挙件数	338	332	462	599	520
	検挙事件数[注8]	141	154	175	216	160
	検挙人員	150	154	192	242	164
識別符号提供（助長）行為	検挙件数	0	5	5	9	4
	検挙事件数	0	5	2	6	4
	検挙人員	0	5	3	12	4
識別符号取得行為	検挙件数	16	10	6	5	22
	検挙事件数	5	1	3	3	1
	検挙人員	15	1	3	5	2
識別符号保管行為	検挙件数	2	12	28	31	16
	検挙事件数	2	2	6	2	9
	検挙人員	2	2	6	6	12
フィッシング行為	検挙件数	8	14	1	4	2
	検挙事件数	6	14	1	3	2
	検挙人員	6	14	1	4	2
計	検挙件数（件）	364	373	502	648	564
	検挙事件数（事件）	150（重複4）	173（重複3）	182（重複5）	227（重複3）	170（重複6）
	検挙人員（人）	170（重複3）	173（重複3）	200（重複5）	255（重複14）	173（重複11）

※　１事件で複数の区分の行為を検挙した場合又は１人の被疑者を複数の区分の行為で検挙した場合は、それぞれの区分に重複して計上。

注4　他人の識別符号をアクセス管理者又は利用権者以外の者に正当な理由なく提供する行為をいう。

注5　不正アクセスの目的で他人の識別符号を取得する行為をいう。

注6　不正アクセスの目的で他人の識別符号を保管する行為をいう。

注7　アクセス管理者になりすまし、当該アクセス制御機能に係る識別符号の入力を求める行為をいう。例えば、フィッシングサイトを公衆が閲覧できる状態に置く行為が該当する。

注8　事件数とは、事件単位ごとに計上した数であり、一連の捜査で複数の件数の犯罪を検挙した場合は１事件と数える。

(2)　不正アクセス行為の手口別検挙状況

不正アクセス行為の検挙件数について手口別に内訳を見ると、「識別符号窃用型[注9]」が502件と約96.5%を占めている。

表２－２　過去５年の不正アクセス行為の手口別検挙件数等

区分＼年次		平成26年	平成27年	平成28年	平成29年	平成30年
識別符号窃用型	検挙件数	336	331	457	545	502
	検挙事件数	140	153	174	213	155
セキュリティ・ホール攻撃型	検挙件数	2	1	5	54	18
	検挙事件数	2	1	3	5	6
計	検挙件数（件）	338	332	462	599	520
	検挙事件数（事件）	141 (重複1)	154	175 (重複2)	216 (重複2)	160 (重複1)

※　１事件で複数の区分の行為を検挙した場合は、それぞれの区分に重複して計上。

注9　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（不正アクセス禁止法第２条第４項第１号に該当する行為）をいう。

3　検挙した不正アクセス禁止法違反事件の特徴

(1)　被疑者等の年齢

検挙した不正アクセス禁止法違反に係る被疑者の年齢は、「14～19歳」と「20～29歳」がそれぞれ48人で、次いで「30～39歳」が37人の順となっている[注10]。

なお、不正アクセス禁止法違反として補導又は検挙された者のうち、最年少の者は11歳[注11]、最年長の者は66歳であった。

図３－１　平成30年における年代別被疑者数

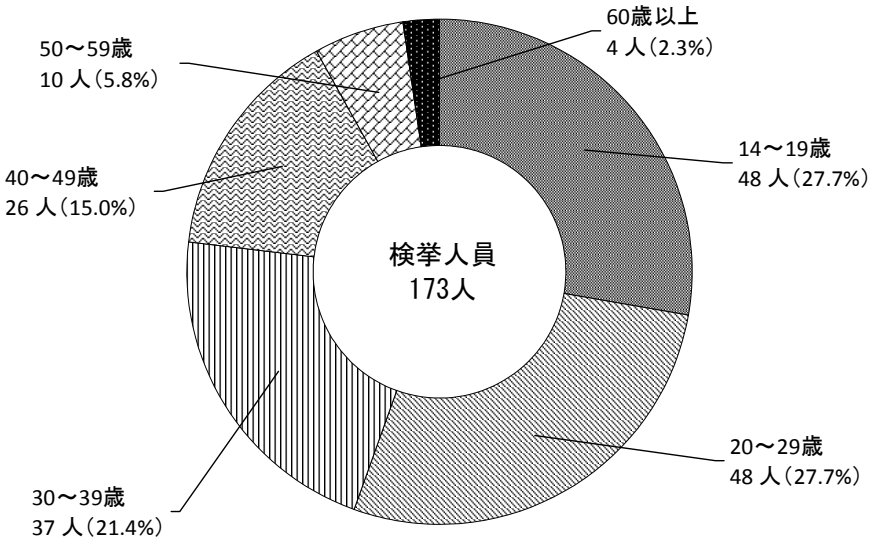


表３－１　過去５年の年代別被疑者数の推移

区分＼年次	平成26年	平成27年	平成28年	平成29年	平成30年
14～19歳	49	53	62	92	48
20～29歳	43	43	56	87	48
30～39歳	45	41	48	36	37
40～49歳	25	29	29	28	26
50～59歳	5	5	3	11	10
60歳以上	3	2	2	1	4
計（人）	170	173	200	255	173

(2)　被疑者と利用権者の関係

不正アクセス禁止法違反に係る被疑者と識別符号を窃用された利用権者との関係をみると、「元交際相手や元従業員等の顔見知りの者によるもの」が最も多く（108人）、次いで「交友関係のない他人によるもの」（53人）、「ネットワーク上の知り合いによるもの」（12人）の順となっている。

注10　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人が触法少年として補導されている（犯罪統計による集計）。

注11　14歳未満の少年であるため、検挙事件及び検挙人員としては計上していない。

(3)　不正アクセス行為の手口

検挙した不正アクセス禁止法違反に係る識別符号窃用型の不正アクセス行為の手口を見ると、「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」が最も多く（278件）、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」（131件）となっており、平成26年と比較するとそれぞれ約3.3倍、約2.8倍となっている。

図３－２　平成30年における不正アクセス行為（識別符号窃用型）に係る手口別検挙件数

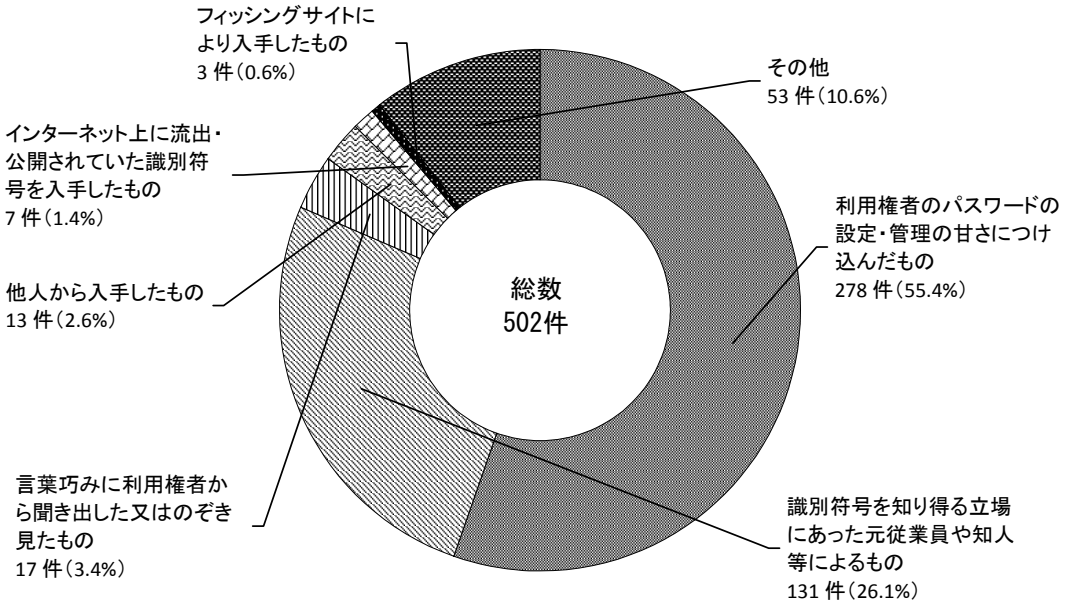


表３－２　過去５年の不正アクセス行為に係る手口別検挙件数

区分＼年次	平成26年	平成27年	平成28年	平成29年	平成30年
識別符号窃用型（件）	336	331	457	545	502
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	84	117	244	230	278
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	47	51	61	113	131
言葉巧みに利用権者から聞き出した又はのぞき見たもの	53	46	49	42	17
他人から入手したもの	25	13	20	74	13
インターネット上に流出・公開されていた識別符号を入手したもの	34	57	4	0	7
フィッシングサイトにより入手したもの	71	24	3	2	3
スパイウェア[注12]等のプログラムを使用して識別符号を入手したもの	6	15	34	37	0
その他	16	8	42	47	53
セキュリティ・ホール攻撃型（件）	2	1	5	54	18

注12　パソコン内のファイル情報、キーボードの入力情報、表示画面の情報等を取り出して、漏えいさせる機能を持つプログラムをいう。

(4)　不正アクセス行為の動機

検挙した不正アクセス禁止法違反に係る不正アクセス行為の動機を見ると、「顧客データの収集等情報を不正に入手するため」が最も多く（195件）、次いで「好奇心を満たすため」（103件）、「オンラインゲームやコミュニティサイトで不正操作を行うため」（101件）の順となっている。

図３－３　平成30年における不正アクセス行為に係る動機別検挙件数

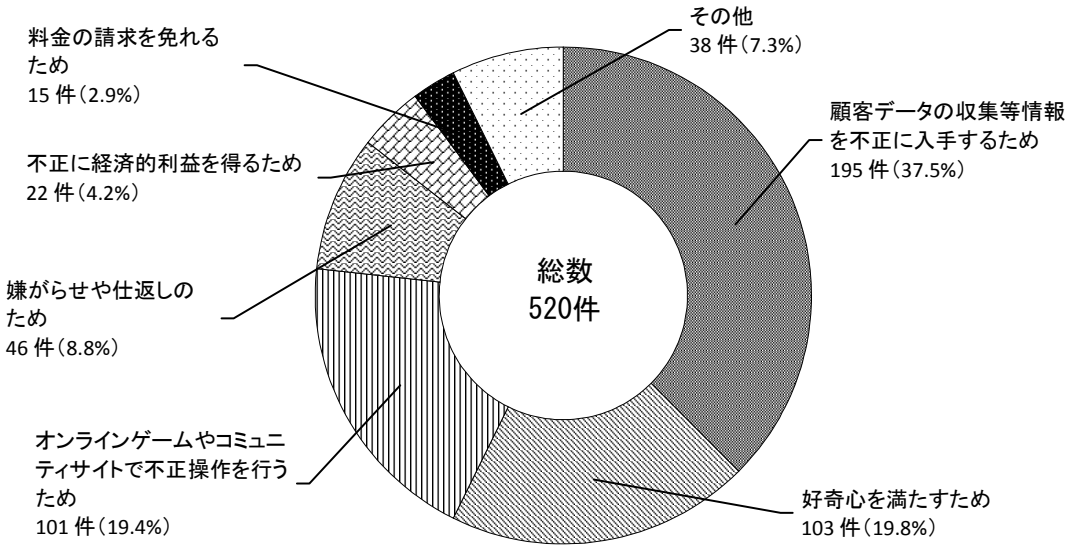


表３－３　過去５年の不正アクセス行為に係る動機別検挙件数

区分＼年次	平成26年	平成27年	平成28年	平成29年	平成30年
顧客データの収集等情報を不正に入手するため	139	72	70	103	195
好奇心を満たすため	15	76	208	193	103
オンラインゲームやコミュニティサイトで不正操作を行うため	41	28	43	43	101
嫌がらせや仕返しのため	54	44	44	59	46
不正に経済的利益を得るため	86	52	41	93	22
料金の請求を免れるため	2	58	25	86	15
その他	1	2	31	22	38
計（件）	338	332	462	599	520

(5)　不正に利用されたサービス

検挙した不正アクセス禁止法違反に係る識別符号窃用型の不正アクセス行為（502件）について、他人の識別符号を用いて不正に利用されたサービス別の内訳を見ると、「オンラインゲーム・コミュニティサイト」が最も多く（217件）、次いで「社員・会員用等の専用サイト」（200件）となっており、平成26年と比較してどちらも約3.1倍になっている。

図３－４　平成30年における不正アクセス行為（識別符号窃用型）に係る不正に利用されたサービス別検挙件数

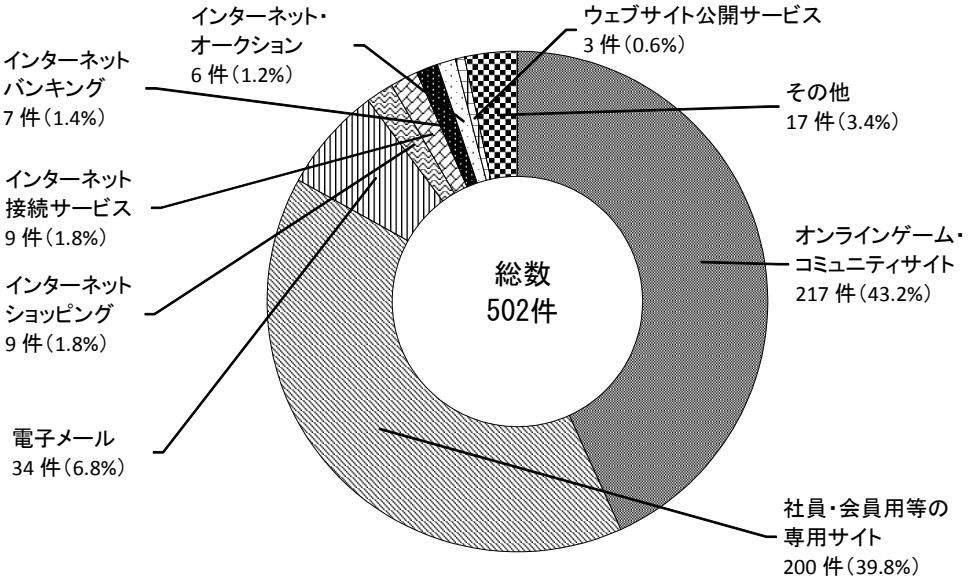


表３－４　過去５年の不正に利用されたサービス別検挙件数

区分＼年次	平成26年	平成27年	平成28年	平成29年	平成30年
識別符号窃用型　（件）	336	331	457	545	502
オンラインゲーム・コミュニティサイト	69	116	185	210	217
社員・会員用等の専用サイト	65	20	40	116	200
電子メール	30	64	136	92	34
インターネットショッピング	44	54	18	22	9
インターネット接続サービス	11	11	5	2	9
インターネットバンキング	20	30	13	8	7
インターネット・オークション	15	20	9	11	6
ウェブサイト公開サービス	7	9	2	7	3
その他	75	7	49	77	17

４　検挙事例

(1)　旅館従業員の男（32）は、平成30年３月、鉄道会社のウェブサイトに対し、サイト管理用のＩＤ・パスワードを使用して不正アクセスし、ウェブサイトのデータを削除して閲覧不能な状態にした。同年10月、不正アクセス禁止法違反（不正アクセス行為）と電子計算機損壊等業務妨害で送致した。（宮崎）

(2)　無職の男（22）は、平成29年２月、国内のインターネットオークションサイトに対し、掲示板サイトから不正に入手したＩＤ・パスワードを使用して不正アクセスし、オークションの商品売買を装って現金を騙し取った。平成30年３月、不正アクセス禁止法違反（不正アクセス行為）、私電磁的記録不正作出・同供用及び詐欺で検挙した。（和歌山）

(3)　会社員の男（39）は、平成30年５月、オンラインゲームのゲーム引継時に利用するサーバに対し、他人のＩＤ・パスワードを使用して不正アクセスし、ゲームデータの引継処理を行い、他人のゲームデータを乗っ取った。同年11月、不正アクセス禁止法違反（不正アクセス行為）と私電磁的記録不正作出・同供用で逮捕した。（福島）

(4)　会社員の男（33）は、平成30年５月、自らが勤務する会社の社内ネットワークに対し、他人のＩＤ・パスワードを使用して不正アクセスし、実行すると本人の意に反してデータを削除するプログラムを蔵置してこれを実行させた。同年６月、不正アクセス禁止法違反（不正アクセス行為）と不正指令電磁的記録供用で逮捕した。（栃木）

(5)　会社員の男（33）は、平成29年４月から８月までの間、ウイルス対策ソフトの管理システムに対し、自らが勤務していた会社に付与された管理用IDとパスワードを使用して不正アクセスし、会社の業務用端末に導入されたウイルス対策ソフトを削除する等した。平成30年５月、不正アクセス禁止法違反（不正アクセス行為）、私用電磁的記録毀棄及び偽計業務妨害で送付した。（神奈川）

第２　防御上の留意事項

１　利用権者の講ずべき措置

(1)　パスワードの適切な設定・管理

利用権者のパスワードの設定・管理の甘さにつけ込んだ手口が多発していることから、パスワードを設定する場合には、ＩＤと同じものや利用権者の名前、電話番号、誕生日等のパスワードの推測が容易なものを避けるほか、複数のサイトで同じＩＤ・パスワードの組合せを使用しないなどの対策を講ずる。また、パスワードを他人に教えないなど、自己のパスワードは適切に管理する。

(2)　フィッシングに対する注意

電子メールやＳＭＳを用いて、本物のウェブサイトに酷似したフィッシングサイトに誘導し、ＩＤ・パスワードやクレジットカード情報を不正に取得する事案が発生していることから、送信元に心当たりのある電子メール等であっても、メールに記載のリンク等が公式のウェブサイトのものと相違ないか確認するなど、フィッシングサイトへの誘導には注意する。

(3)　不正に用いられるプログラムに対する注意

コンピュータにプログラムを不正に感染させ、他人のＩＤ・パスワードを不正に取得する事案も発生していることから、心当たりのある企業からの電子メールであっても、正当な電子メールと判断できるまでは添付ファイルを開かないことや、電子メールに記載のリンクをクリックしないことを徹底するとともに、不特定多数が利用するコンピュータではクレジットカード情報等の重要な情報を入力しないことも徹底する。また、不正に用いられるプログラムへの対策（ウイルス対策ソフトの利用のほか、オペレーティングシステムやウイルス対策ソフトを含む各種ソフトウェアのアップデート等）を適切に講ずる。特に、インターネットバンキング、仮想通貨の取引、インターネットショッピング、オンラインゲーム等の利用に際しては、セキュリティ対策ソフトを利用するとともに、ワンタイムパスワード[注13]又は二経路認証[注14]・二要素認証[注15]を導入するなどの金融機関等が推奨するセキュリティ対策を積極的に利用する。

２　アクセス管理者の講ずべき措置

(1)　パスワードの適切な設定・運用体制の構築

利用権者のパスワードの設定・管理の甘さにつけ込んだ不正アクセス行為が多発していることから、文字数や使用文字に条件を付けるなど、容易に推測されるパスワードを設定できないようにすることのほか、複数のサイトで同じＩＤ・パスワードの組合せを使用することの危険性を周知するなどの措置を講ずる。

また、正規利用権者が通常使用するＩＰアドレスや時間帯等と異なる不審なログインを早期に検知する体制を構築する。

(2)　ＩＤ・パスワードの適切な管理

元従業員や委託先業者等ＩＤ・パスワードを知り得る立場にあった者による不正

注13　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をいう。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。

注14　インターネットバンキング等において、パーソナルコンピュータ（第一経路）で振り込み等の取引データを作成した後、スマートフォン等（第二経路）で承認を行うことで取引を成立させる認証方式をいう。

注15　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。

アクセス行為が発生していることから、利用権者が特定電子計算機を利用する立場でなくなったときには、当該者に割り当てていたＩＤを削除したり、パスワードを変更したりするなど、ＩＤ・パスワードの適切な管理を徹底する。

(3)　フィッシング等への対策

フィッシング等により取得したＩＤ・パスワードを用いて不正アクセス行為を行う事案が発生しているほか、フィッシング等によって不正に取得された可能性があるＩＤ・パスワードがインターネット上に流出・公開される事例もあることから、ワンタイムパスワード又は二経路認証・二要素認証の導入等により認証を強化する。

(4)　セキュリティ・ホール攻撃への対応

ＳＱＬインジェクション[注17]攻撃、ウェブサーバの脆弱性に対する攻撃等のセキュリティ・ホール攻撃への対策として、定期的にウェブサーバのプログラムを点検してセキュリティ上の脆弱性を解消するとともに、攻撃の兆候を即座に検知するためのシステムを導入するなど、セキュリティ・ホール攻撃に対する監視体制を強化する。

注17　ＳＱＬというプログラム言語を用いて、企業等が個人情報を管理するデータベースを外部から不正に操作する行為をいう。

（参考）　不正アクセス関連行為の関係団体への届出状況について

○　独立行政法人情報処理推進機構（IPA）に届出のあったコンピュータ不正アクセスの届出状況について

平成30年１月１日から12月31日の間にIPAに届出のあったコンピュータ不正アクセス（注１）が対象である。

コンピュータ不正アクセスに関する届出件数は54件（平成29年：79件）であった。（注２）

平成30年は同29年と比べて、25件（約31.6%）減少した。

届出のうち実際に被害があったケースにおける被害内容の分類では､「なりすまし」による被害届出が多く寄せられた。

以下に、種々の切り口で分類した結果を示す。個々の件数には未遂（実際の被害はなかったもの）も含まれる。また、１件の届出にて複数の項目に該当するものがあるため、それぞれの分類での総計件数はこの数字に必ずしも一致しない。

(1) 手口別分類

意図的に行う攻撃行為による分類である。１件の届出について複数の攻撃行為を受けている場合もあるため、届出件数とは一致せず総計は73件（平成29年：87件）となる。

ア　侵入行為に関して

侵入行為に係る攻撃等の届出は33件（平成29年：55件）あった。

(ｱ) 侵入の事前調査行為

システム情報の調査、稼働サービスの調査、アカウント名の調査等である。

２件の届出があり、ポートやセキュリティホールを探索するものと総当たり攻撃によるアカウント名の調査であった。

(ｲ) 権限取得行為（侵入行為）

パスワード推測やソフトウェアのバグ等いわゆるセキュリティホールを利用した攻撃やシステムの設定内容を利用した攻撃等侵入のための行為である。

18件の届出があり、これらのうち実際に侵入につながったものは15件である。

【主な内容】

パスワード推測：13件

(ｳ) 不正行為の実行及び目的達成後の行為

侵入その他、何らかの原因により不正行為を実行されたことについては13件の届出があった。

【主な内容】

ファイル等の改ざん、破壊等：３件

プログラムの作成・設置（インストール）、トロイの木馬等の埋め込み等：５件

イ　サービス妨害攻撃

過負荷を与えたり、例外処理を利用してサービスを不可若しくは低下させたりする攻撃で、11件（平成29年：12件）の届出があった。

ウ　その他

その他にはメール不正中継やメールアドレス詐称、正規ユーザになりすましてのサービスの不正利用、ソーシャルエンジニアリング等が含まれ、29件（平成29年：20件）の届出があった。

【主な内容】

正規ユーザへのなりすまし：18件

メールアドレス詐称：１件

(2) 原因別分類

不正アクセスを許した問題点／弱点による分類である。

54件の届出中、実際に被害に遭った計43件（平成29年：54件）を分類すると次のようになる。

被害原因として「ID、パスワード管理不備」が多く、パスワードの使い回しやフィッシング、初期値のままでの利用など、アカウント所有者のパスワード管理の隙を狙った攻撃が多いと推測される。また、原因が不明なケースも依然として少なくはなく、手口の巧妙化により原因の特定に至らない事例が多いと推測される。

【主な要因】

ID、パスワード管理の不備によると思われるもの：23件

設定の不備（セキュリティ上問題のあるデフォルト設定を含む。）によるもの：７件

DoS攻撃：４件

原因不明：８件

(3) 電算機分類

不正アクセス行為の対象となった機器による分類である（被害の有無は問わない。）。

【主な対象】

WWW サーバ：19 件
メールサーバ：14 件
ファイアウォール：４件
不明：６件
※１件の届出で複数の項目に該当するものがある。

(4) 被害内容分類

54 件の届出を被害内容で分類した 63 件中、実際に被害に遭ったケースにおける被害内容による分類である。機器に対する実被害があった件数は 47 件（平成 29 年：52 件）である。

なお、対処に係る工数やサービスの一時停止、代替機の準備等に関する被害は除外している。

【主な被害内容】

踏み台として悪用：13 件
オンラインサービスの不正利用：10 件
データの窃取や盗み見：９件
ホームページ改ざん：５件
サービス低下：５件
※１件の届出で複数の項目に該当するものがある。

(5) 対策情報

平成 30 年はなりすまし被害の届出が多く、メールアカウントに不正ログインされ、スパムメールやばらまき型メールの踏み台として悪用される被害が多く見られた。また平成 29 年に引き続き、BEC（ビジネスメール詐欺）の被害も見られた。メールに関する被害の他に、近年普及してきた仮想通貨について、サーバにマイニングプログラムが埋め込まれるという資源の不正利用に関する被害も見られた。これらを含む不正アクセス届出において、被害に遭った 43 件のうち「ID、パスワード管理の不備」が原因とされる届出は 24 件（約 55.8%）と、依然大きな割合を占めている。パスワードの管理が適切でない場合、サーバの脆弱性を解消していてもウェブサイトを改ざんされたり、スパムメール送信の踏み台とされたりといった被害を防ぐことはできないため、以下のような対策が必要となる。

システム管理者向け対策

・　ログイン通知やログイン履歴の機能を設ける
・　外部からメールサーバへ接続する際にはアカウント情報以外の認証情報を必要とする

など、不正ログインを早急に検知できたり、二段階認証となるような機能追加を検討することが推奨される。

ユーザの対策

・　他者に推測されにくい複雑なパスワードを設定する
・　パスワードの使いまわしをしない
・　二段階認証などのセキュリティオプションを積極的に採用する

など、適切なアカウント管理とリスクへの対策を実施することが推奨される。

下記ページ等を参照し、今一度状況確認・対処されたい。

【システム管理者向け】

「安全なウェブサイトの作り方　改訂第７版」
https://www.ipa.go.jp/security/vuln/websecurity.html

「JVN（Japan Vulnerability Notes)」　※脆弱性対策情報ポータルサイト
https://jvn.jp/

「IPA メールニュース」
https://www.ipa.go.jp/about/mail/

【個人ユーザ向け】

「ここからセキュリティ」情報セキュリティ・ポータルサイト
https://www.ipa.go.jp/security/kokokara/

「IPA セキュリティセンター・個人ユーザ向けページ」
https://www.ipa.go.jp/security/personal/index.html

「MyJVN」（セキュリティ設定チェッカ、バージョンチェッカ）
https://jvndb.jvn.jp/apis/myjvn/

ウイルス対策を含むセキュリティ関係の情報・対策等については、下記ページを参照のこと。

「IPA セキュリティセンタートップページ」
https://www.ipa.go.jp/security/

注１　コンピュータ不正アクセス

システムを利用する者が、その者に与えられた権限によって許された行為以外の行為を、ネットワークを介して意図的に行うこと。

注２　ここに挙げた件数は、コンピュータ不正アクセスの届出を IPA が受理した件であり、不正アクセスやアタック等に関して実際の発生件数や被害件数を直接類推できるような数値ではない。

○　一般社団法人 JPCERT コーディネーションセンター（以下、JPCERT/CC）に報告があった不正アクセス関連行為の状況について

JPCERT/CC は、国内の情報セキュリティインシデントの被害低減を目的として、広く一般から不正アクセス関連行為を含むコンピュータセキュリティインシデントに関する調整対応依頼を受け付けている。

１．　不正アクセス関連行為の特徴および件数

（平成 30 年 1 月 1 日から 12 月 31 日の間に JPCERT/CC に報告（調整対応依頼）のあったコンピュータ不正アクセスが対象）

報告（調整対応依頼）のあった不正アクセス関連行為(注１)に係わる報告件数(注２)は 15,751 件であった。この報告を元にしたインシデント件数（注３）は 15,351 件であり、インシデントをカテゴリ別に分類すると以下の通りである。

（１）　プローブ、スキャン、その他不審なアクセスに関する報告

防御に成功したアタックや、コンピュータ／サービス／弱点の探査を意図したアクセス、その他の不審なアクセス等、システムのアクセス権において影響を生じないか、無視できるアクセスについて 5,941 件の報告があった。
[1/1-3/31:1,845 件、4/1-6/30:1,255 件、7/1-9/30:1,164 件、10/1-12/31: 1,677 件]

（２）　Web サイト改ざん

攻撃者もしくはマルウエアによって､Web サイトのコンテンツが書き換えられたサイトについて 1,056 件の報告があった。
[1/1-3/31: 268 件、4/1-6/30: 320 件、7/1-9/30: 226 件、10/1-12/31: 242 件]

（３）　マルウエアサイト

閲覧することで PC がマルウエアに感染してしまう攻撃用サイトや攻撃に使用するマルウエアを公開しているサイトについて 325 件の報告があった。
[1/1-3/31:63 件、4/1-6/30: 89 件、7/1-9/30: 98 件、10/1-12/31: 75 件]

（４）　ネットワークやコンピュータの運用を妨害しようとする攻撃

大量のパケットや予期しないデータの送信によって、サイトのネットワークやホストのサービス運用を妨害しようとするアクセスについて 18 件の報告があった。

[1/1-3/31: 1 件、4/1-6/30: 0 件、7/1-9/30: 10 件、10/1-12/31: 7 件]

（５） Web 偽装事案(phishing)

Web のフォームなどから入力された口座番号やキャッシュカードの暗証番号といった個人情報を盗み取る Web 偽装事案について 5,000 件の報告があった。

[1/1-3/31:924 件、4/1-6/30: 1,214 件、7/1-9/30: 1,302 件、10/1-12/31: 1,560 件]

（６） 制御システム関連

インターネット経由で攻撃が可能な制御システム等について 7 件の報告があった。

[1/1-3/31: 7 件、4/1-6/30: 0 件、7/1-9/30: 0 件、10/1-12/31: 0 件]

（７）標的型攻撃

特定の組織、企業、業種などを標的として、マルウエア感染や情報の窃取などを試みる攻撃について 26 件の報告があった。

[1/1-3/31: 6 件、4/1-6/30: 9 件、7/1-9/30: 7 件、10/1-12/31: 4 件]

（８） その他

コンピュータウイルス、SPAM メールの受信等について 2,978 件の報告があった。

[1/1-3/31: 743 件、4/1-6/30: 708 件、7/1-9/30: 604 件、10/1-12/31: 923 件]

２． 防御に関する啓発および対策措置の普及

JPCERT/CC は、日本国内のインターネット利用者に対して、不正アクセス関連行為を防止するための予防措置や、発生した場合の緊急措置などに関する情報を提供し、不正アクセス関連行為への認識の向上や適切な対策を促進するため、以下の文書を公開している(詳細は http://www.jpcert.or.jp/参照。)

（１） 注意喚起

[新規]

2018 年 1 月	Adobe Flash Player の脆弱性 (APSB18-01) に関する注意喚起 2018 年 1 月マイクロソフトセキュリティ更新プログラムに関する

	注意喚起 2018 年 1 月 Oracle Java SE のクリティカルパッチアップデートに関する注意喚起 Oracle WebLogic Server の脆弱性（CVE-2017-10271）に関する注意喚 ISC BIND 9 の脆弱性に関する注意喚起
2018 年 2 月	Adobe Flash Player の未修正の脆弱性（CVE-2018-4878）に関する注意喚起 2018 年 2 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 memcached のアクセス制御に関する注意喚起
2018 年 3 月	Mirai 亜種の感染活動に関する注意喚起 Adobe Flash Player の脆弱性（APSB18-05）に関する注意喚起 2018 年 3 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 Drupal の脆弱性（CVE-2018-7600）に関する注意喚起
2018 年 4 月	Cisco Smart Install Client を悪用する攻撃に関する注意喚起 Spring Framework の脆弱性に関する注意喚起 Adobe Flash Player の脆弱性（APSB18-08）に関する注意喚起 2018 年 4 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 Drupal の脆弱性（CVE-2018-7600）に関する注意喚起 Spring Data Commons の脆弱性に関する注意喚起 2018 年 4 月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起 Drupal の脆弱性（CVE-2018-7602）に関する注意喚起
2018 年 5 月	Adobe Flash Player の脆弱性（APSB18-16）に関する注意喚起 2018 年 5 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 Adobe Reader および Acrobat の脆弱性（APSB18-09）に関する注意喚起 メールクライアントにおける OpenPGP および S/MIME のメッセージの取り扱いに関する注意喚起
2018 年 6 月	Adobe Flash Player の脆弱性（APSB18-19）に関する注意喚起 2018 年 6 月マイクロソフトセキュリティ更新プログラムに関する注意喚起

2018 年 7 月	Adobe Reader および Acrobat の脆弱性（APSB18-21）に関する注意喚起 Adobe Flash Player の脆弱性（APSB18-24）に関する注意喚起 2018 年 7 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 2018 年 7 月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起 Apache Tomcat における複数の脆弱性に関する注意喚起 2018 年 7 月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起
2018 年 8 月	ISC BIND 9 サービス運用妨害の脆弱性（CVE-2018-5740）に関する注意喚起 Adobe Reader および Acrobat の脆弱性（APSB18-29）に関する注意喚起 Adobe Flash Player の脆弱性（APSB18-25）に関する注意喚起 2018 年 8 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 Ghostscript の -dSAFER オプションの脆弱性に関する注意喚起 Apache Struts 2 の脆弱性（S2-057）に関する注意喚起
2018 年 9 月	Adobe Flash Player の脆弱性（APSB18-31）に関する注意喚起 2018 年 9 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 Adobe Reader および Acrobat の脆弱性（APSB18-34）に関する注意喚起
2018 年 10 月	Adobe Acrobat および Reader の脆弱性（APSB18-30）に関する注意喚起 2018 年 10 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 2018 年 10 月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起 Cisco Webex Meetings Desktop App および Cisco Webex Productivity Tools の脆弱性（CVE-2018-15442）に関する注意喚起
2018 年 11 月	Adobe Flash Player の脆弱性（APSB18-39）に関する注意喚起 Adobe Acrobat および Reader の脆弱性（APSB18-40）に関する注意喚起

	2018 年 11 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 Adobe Flash Player の脆弱性（APSB18-44）に関する注意喚起
2018 年 12 月	Adobe Flash Player の脆弱性（APSB18-42）に関する注意喚起 Adobe Acrobat および Reader の脆弱性（APSB18-41）に関する注意喚起 2018 年 12 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 Microsoft Internet Explorer の脆弱性（CVE-2018-8653）に関する注意喚起

（２） 活動概要（報告状況等の公表）

発行日：2018-01-16［ 2017 年 10 月 1 日 ～ 2017 年 12 月 31 日］
発行日：2018-04-12［ 2018 年 1 月 1 日 ～ 2018 年 3 月 31 日］
発行日：2018-07-12［ 2018 年 4 月 1 日 ～ 2018 年 6 月 30 日］
発行日：2018-10-16［ 2018 年 7 月 1 日 ～ 2018 年 9 月 30 日］

（３） JPCERT/CC レポート

[発行件数] 50 件
[取り扱ったセキュリティ関連情報数]343 件

注１　不正アクセス関連行為とは、コンピュータやネットワークのセキュリティを侵害する人為的な行為で、意図的(または、偶発的) に発生する全ての事象が対象になる。

注２　ここにあげた件数は、JPCERT/CC が受け付けた報告の件数である。実際のアタックの発生件数や、被害件数を類推できるような数値ではない。また類型ごとの実際の発生比率を示すものでもない。一定以上の期間に渡るアクセスの要約レポートも含まれるため、アクセスの回数と報告件数も一般に対応しない。報告元には、国内外のサイトが含まれる。

注３　「インシデント件数」は、各報告に含まれるインシデント件数の合計を示す。ただし、1 つのインシデントに関して複数件の報告がよせられた場合は、1 件のインシデントとして扱う。