不正アクセス行為の発生状況

第１　令和元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

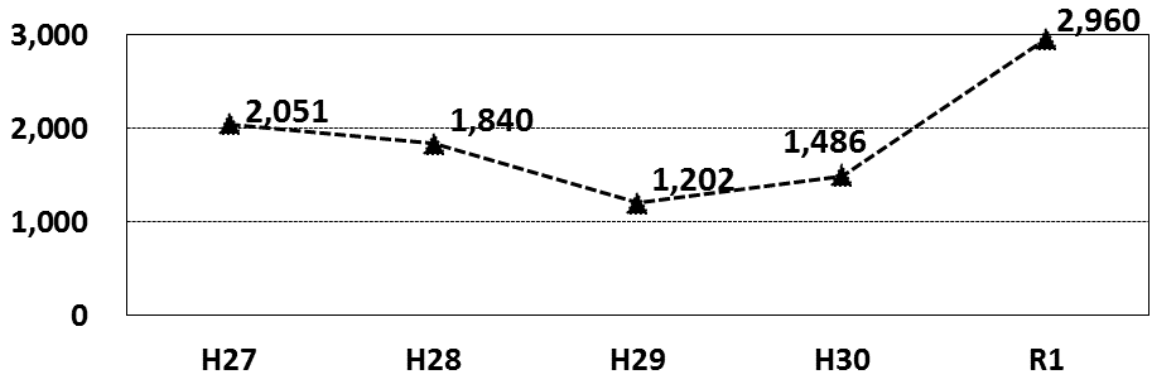
令和元年[注1]に都道府県警察から警察庁に報告のあった不正アクセス行為を対象とした。

１　不正アクセス行為の認知状況

(1)　認知件数

令和元年における不正アクセス行為の認知件数[注2]は2,960件であり、前年と比較すると1,474件（約99.2%）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3]別に内訳を見ると、「一般企業」が最も多く2,855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27年	平成28年	平成29年	平成30年	令和元年
一般企業	1,998	1,823	1,177	1,314	2,855
行政機関等	14	5	9	6	90
プロバイダ	11	6	6	4	6
大学、研究機関等	11	2	5	161	3
その他	17	4	5	1	6
計(件)	2,051	1,840	1,202	1,486	2,960

※「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　令和元年の各種数値については、平成31年１月から同年４月までの数を含む。

注2　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3　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、「警察活動」が最も多く（1,555件）、次いで「利用権者[注4]からの届出」（761件）、「アクセス管理者からの届出」（602件）の順となっている。

図１－２　令和元年における認知の端緒別認知件数

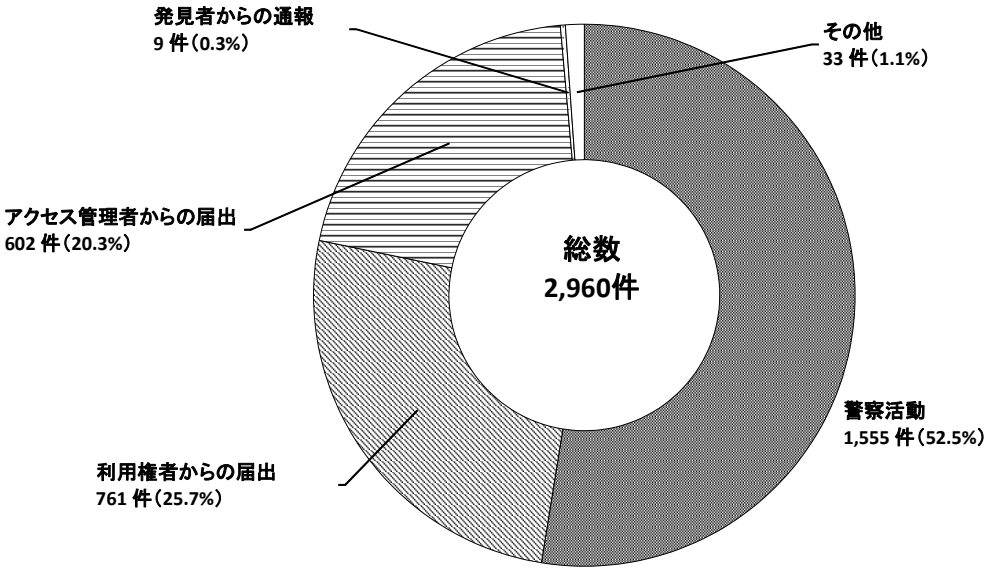


表１－２　過去５年の認知の端緒別認知件数

区分＼年次	平成27年	平成28年	平成29年	平成30年	令和元年
警察活動	516	511	283	269	1,555
利用権者からの届出	614	495	655	852	761
アクセス管理者からの届出	910	828	255	345	602
発見者からの通報	11	5	6	16	9
その他	0	1	3	4	33
計（件）	2,051	1,840	1,202	1,486	2,960

注4　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、「インターネットバンキングでの不正送金等」が前年から約5.5倍に増加して最も多く（1,808件）、次いで「インターネットショッピングでの不正購入」（376件）、「メールの盗み見等の情報の不正入手」（329件）の順となっている。

図１－３　令和元年における不正アクセス後の行為別認知件数

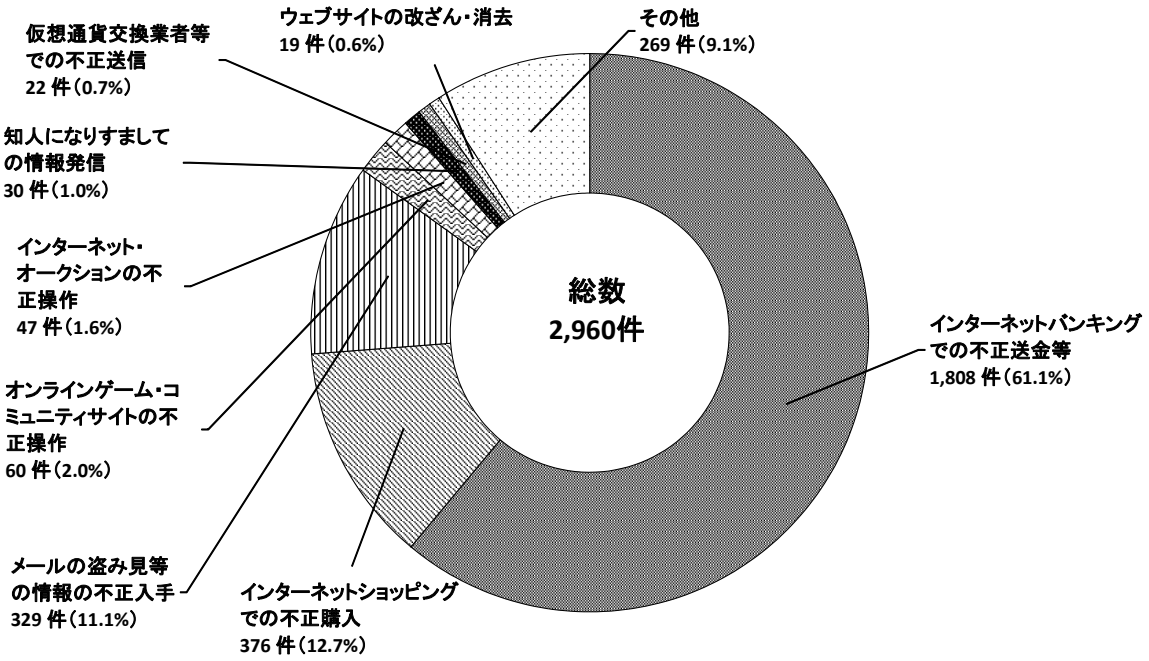


表１－３　過去５年の不正アクセス後の行為別認知件数

区分＼年次	平成27年	平成28年	平成29年	平成30年	令和元年
インターネットバンキングでの不正送金等	1,531	1,305	442	330	1,808
インターネットショッピングでの不正購入	167	172	133	149	376
メールの盗み見等の情報の不正入手	92	91	146	385	329
オンラインゲーム・コミュニティサイトの不正操作	96	124	83	199	60
インターネット・オークションの不正操作	20	34	28	29	47
知人になりすましての情報発信	83	25	110	24	30
仮想通貨交換業者等での不正送信			149	169	22
ウェブサイトの改ざん・消去	34	6	14	13	19
その他	28	83	97	188	269
計（件）	2,051	1,840	1,202	1,486	2,960

※　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

令和元年における不正アクセス禁止法違反の検挙件数は816件、検挙人員は234人であり、前年と比べ、検挙件数は252件、検挙人員は61人増加した。

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787件、222人といずれも９割を超えており、他の類型については「識別符号の取得行為[注5]」が５件、４人、「識別符号の提供（助長）行為[注6]」が９件、９人、「識別符号の保管行為[注7]」が13件、７人、「識別符号の不正要求行為[注8]」が２件、１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27年	平成28年	平成29年	平成30年	令和元年
不正アクセス行為	検挙件数	332	462	599	520	787
	検挙事件数[注9]	154	175	216	160	218
	検挙人員	154	192	242	164	222
識別符号取得行為	検挙件数	10	6	5	22	5
	検挙事件数	1	3	3	1	4
	検挙人員	1	3	5	2	4
識別符号提供（助長）行為	検挙件数	5	5	9	4	9
	検挙事件数	5	2	6	4	6
	検挙人員	5	3	12	4	9
識別符号保管行為	検挙件数	12	28	31	16	13
	検挙事件数	2	6	2	9	5
	検挙人員	2	6	6	12	7
識別符号不正要求行為	検挙件数	14	1	4	2	2
	検挙事件数	14	1	3	2	1
	検挙人員	14	1	4	2	1
計	検挙件数（件）	373	502	648	564	816
	検挙事件数（事件）	173（重複3）	182（重複5）	227（重複3）	170（重複6）	232（重複2）
	検挙人員（人）	173（重複3）	200（重複5）	255（重複14）	173（重複11）	234（重複9）

※　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　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7　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8　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、ＩＤ・パスワードの入力を求める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9　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10]」が785件と約99.7%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27年	平成28年	平成29年	平成30年	令和元年
識別符号窃用型	検挙件数	331	457	545	502	785
	検挙事件数	153	174	213	155	216
セキュリティ・ホール攻撃型	検挙件数	1	5	54	18	2
	検挙事件数	1	3	5	6	2
計	検挙件数（件）	332	462	599	520	787
	検挙事件数（事件）	154	175（重複2）	216（重複2）	160（重複1）	218

※　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（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、「20～29歳」が93人で最も多く、次いで「14～19歳」が55人、「30～39歳」が50人の順となっている[注11]。

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12歳[注12]、最年長の者は62歳であった。

図３－１令和元年における年代別被疑者数

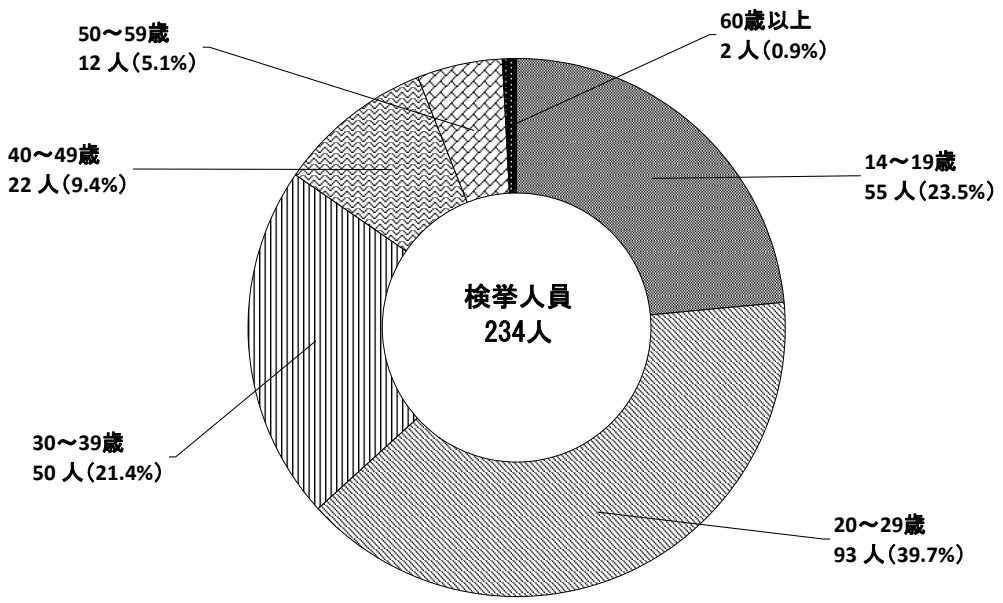


表３－１　過去５年の年代別被疑者数の推移

区分＼年次	平成27年	平成28年	平成29年	平成30年	令和元年
14～19歳	53	62	92	48	55
20～29歳	43	56	87	48	93
30～39歳	41	48	36	37	50
40～49歳	29	29	28	26	22
50～59歳	5	3	11	10	12
60歳以上	2	2	1	4	2
計（人）	173	200	255	173	234

(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（127人）、次いで「交友関係のない他人によるもの」（91人）、「ネットワーク上の知り合いによるもの」（16人）の順となっている。

注11　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６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12　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（310件）、次いで「他人から入手したもの」（182件）となっており、前年と比較するとそれぞれ約1.1倍、14倍となっている。

図３－２　令和元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

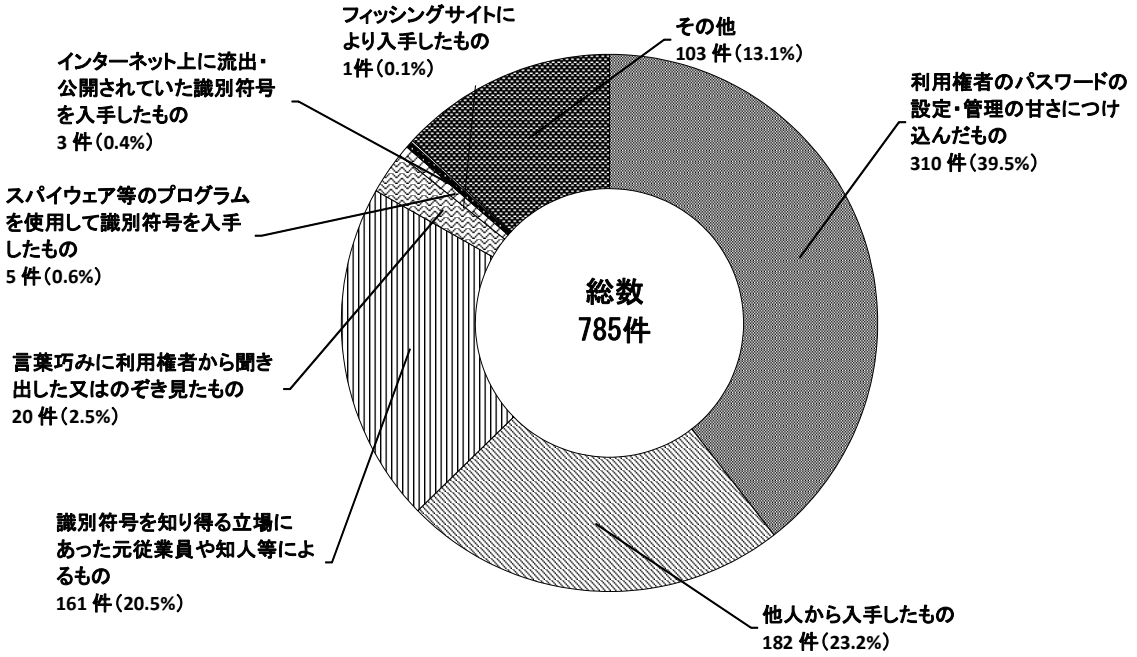


表３－２　過去５年の不正アクセス行為に係る手口別検挙件数

区分＼年次	平成27年	平成28年	平成29年	平成30年	令和元年
識別符号窃用型（件）	331	457	545	502	785
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	117	244	230	278	310
他人から入手したもの	13	20	74	13	182
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	51	61	113	131	161
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	46	49	42	17	20
スパイウェア[注13]等のプログラムを使用して識別符号を入手したもの	15	34	37	0	5
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	57	4	0	7	3
フィッシングサイトにより入手したもの	24	3	2	3	1
その他	8	42	47	53	103
セキュリティ・ホール攻撃型（件）	1	5	54	18	2

注13　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、「不正に経済的利益を得るため」が最も多く（333件）、次いで「顧客データの収集等情報を不正に入手するため」（254件）、「嫌がらせや仕返しのため」（68件）の順となっている。

図３－３　令和元年における不正アクセス行為に係る動機別検挙件数

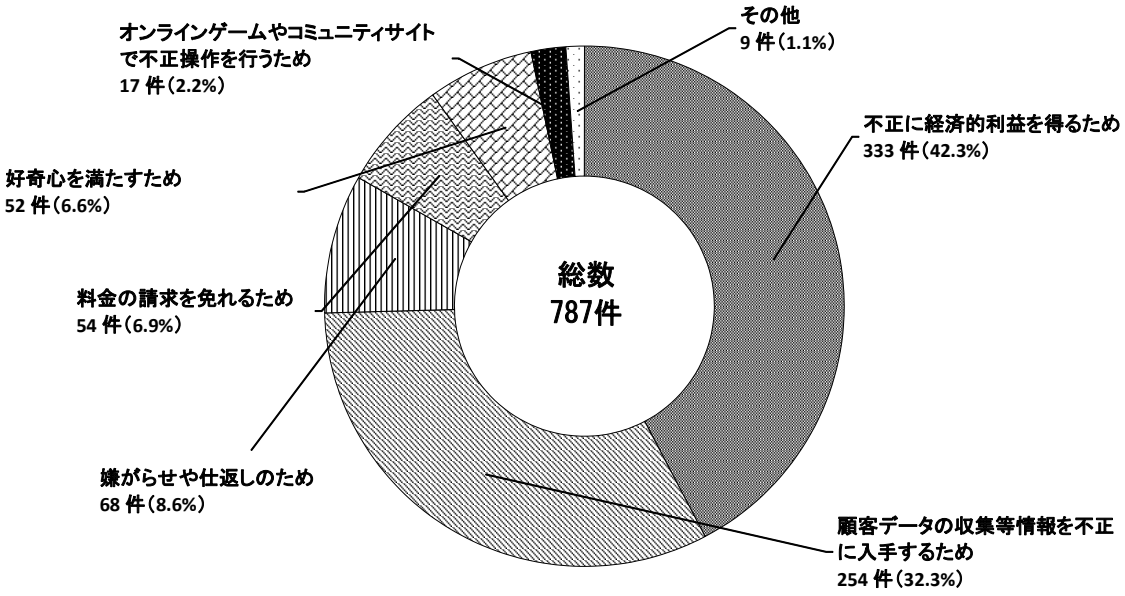


表３－３　過去５年の不正アクセス行為に係る動機別検挙件数

区分＼年次	平成27年	平成28年	平成29年	平成30年	令和元年
不正に経済的利益を得るため	52	41	93	22	333
顧客データの収集等情報を不正に入手するため	72	70	103	195	254
嫌がらせや仕返しのため	44	44	59	46	68
料金の請求を免れるため	58	25	86	15	54
好奇心を満たすため	76	208	193	103	52
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	28	43	43	101	17
その他	2	31	22	38	9
計（件）	332	462	599	520	787

(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（785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（224件）、次いで「社員・会員用等の専用サイト」（151件）となっており、前年と比較すると、それぞれ横ばい、24.5%の減少となっている。

図３－４　令和元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

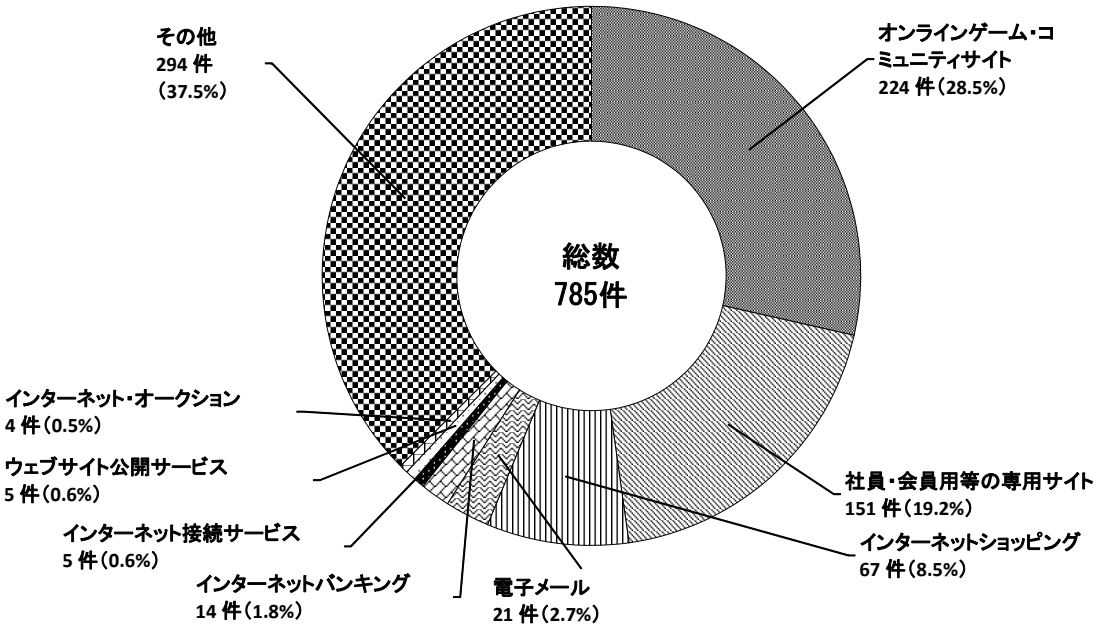


表３－４　過去５年の不正に利用されたサービス別検挙件数

区分＼年次	平成27年	平成28年	平成29年	平成30年	令和元年
識別符号窃用型　（件）	331	457	545	502	785
オンラインゲーム・コミュニティサイト	116	185	210	217	224
社員・会員用等の専用サイト	20	40	116	200	151
インターネットショッピング	54	18	22	9	67
電子メール	64	136	92	34	21
インターネットバンキング	30	13	8	7	14
インターネット接続サービス	11	5	2	9	5
ウェブサイト公開サービス	9	2	7	3	5
インターネット・オークション	20	9	11	6	4
その他	7	49	77	17	294

４　検挙事例

(1)　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、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。（栃木）

(2)　外国人留学生の男(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、他人のアカウント保管の換金可能な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、不正アクセス禁止法違反（不正アクセス行為）と電子計算機使用詐欺で逮捕した。（千葉）

(3)　中国国籍の男(29)は、令和元年７月、不正に取得したＩＤ・パスワードを使用して、コード決済システムに不正アクセスし、コンビニエンスストアにおいて、電子タバコカートリッジを騙し取った。同年10月、不正アクセス禁止法違反（不正アクセス行為）と詐欺罪で逮捕した。（熊本）

(4)　公務員の男(50)は、平成29年１月から平成31年２月までの間、勤務先の同僚のＩＤ・パスワードを無断で使用し、公務用サーバに不正アクセスし、同サーバ内のデータを不正に入手した。令和元年９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。（長崎）

(5)　会社員の男(31)は、令和元年５月、勤務先の同僚のＩＤ・パスワードを無断で使用し、勤務先の福利厚生サイトに不正アクセスした上、同僚のアカウント保管のポイントを使用し、ギフト券を購入した。令和元年11月、不正アクセス禁止法違反（不正アクセス行為）と電子計算機使用詐欺で逮捕した。（静岡）

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発生していることから、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

実在する企業を装ったフィッシングサイトへ誘導するメールやＳＭＳ（ショートメッセージサービス）が多数確認されていることから、このようなメールやＳＭＳに記載されたリンクからアクセスしたサイトにＩＤ・パスワード等を入力しない。

(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14]又は二経路認証[注15]・二要素認証[注16]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)　運用体制の構築

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)　パスワードの適切な設定

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発生していることから、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。

(3)　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14　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15　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16　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。

(4)　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・パスワード等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ほか、自らが管理する特定電子計算機に係るフィッシング等の情報を収集し、利用者に注意喚起を行うなどの措置を講ずる。

(5)　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

令和元年(平成31年１月１日から令和元年12月31日までの１年間。以下同じ。)に IPA に届出のあったコンピュータ不正アクセス（注１）の件数は 89 件（平成30 年：54 件）であった。（注２）

令和元年は平成 30 年と比べて、35 件（約 64.8%）増加した。

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 89 件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 126 件（平成 30 年：73 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 59 件（平成 30 年：33 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。

４件の届出があり、ポートを探索するものと不正入手したアカウントとパスワードによるオンラインサービスのアカウント名の調査等である。

(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の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による侵入のための行為である。

23 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 16 件である。

【主な内容】

パスワード推測：10 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39件の届出があった。

【主な内容】

ファイル等の改ざん、破壊等：28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：９件

イ サービス妨害攻撃

過負荷を与えたり、例外処理を利用したり、サービスを不可又は低下させたりする攻撃で、12件（平成30年：11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、55件（平成30年：29件）の届出があった。

【主な内容】

正規ユーザへのなりすまし：21件

スパムメール：７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。

89件の届出中、実際に被害に遭った計56件（平成30年：43件）を分類すると次のようになる。

被害原因として「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。）」が多いが、これは、サーバ側のアクセス制限を行っていなかった等、セキュリティ上問題のあるデフォルト設定の隙を狙った攻撃が多いためであると推測される。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】

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：15件

原因不明：15件

ID、パスワード管理の不備によると思われるもの：９件

古いバージョンの利用や、パッチ・必要なプラグイン等の未導入によるもの：７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：29 件
メールサーバ：６件
クライアント：６件
不明：４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

89 件の届出を被害内容で分類すると 123 件となるが、そのうち、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 82 件（平成 30 年：47 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】

データの窃取や盗み見：28 件
オンラインサービスの不正利用：19 件
ファイルの書き換え：８件
踏み台として悪用：７件
ホームページ改ざん：６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

令和元年はなりすましによる被害の届出が依然として多く見られる一方で、EC サイトの改ざんによるクレジットカード情報の窃取や DB サーバへの不正アクセスによるデータの消去といった各種サーバに対する被害の届出も見られた。これらサーバに対する不正アクセスの原因として、ウェブサイトの構築・運用に用いられる CMS（コンテンツマネジメントシステム）の設定不備や古いバージョンの利用等が見られた。被害に遭った 60 件のうち「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。）」と「古いバージョンの利用や、パッチ・必要なプラグイン等の未導入によるもの」が原因とされる届出を合わせると 22 件（約 36.7%）と大きな割合を占めている。

ウェブサイト等のサーバへの不正アクセスを防ぐためには、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 としては、
・ ウェブアプリケーションの定期的な脆弱性対策の実施
・ ウェブサーバ上の不要なサービスの停止
など、ウェブサイトのセキュリティホールを無くしていくことが推奨される。

また、ユーザの対策 としては、
・ 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運用管理に向けての 20 ヶ条
～セキュリティ対策のチェックポイント～」
https://www.ipa.go.jp/security/vuln/websitecheck.html
「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/index.html

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

令和元年（平成 31 年 1 月 1 日から令和元年 12 月 31 日までの１年間）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 18,070 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 20,303 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 5,052 件の報告があった。
[1/1-3/31: 2,165 件、4/1-6/30: 1216 件、7/1-9/30: 927 件、10/1-12/31: 744 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 1,013 件の報告があった。
[1/1-3/31: 229 件、4/1-6/30: 256 件、7/1-9/30: 236 件、10/1-12/31: 292 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 902 件の報告があった。
[1/1-3/31: 136 件、4/1-6/30: 292 件、7/1-9/30: 269 件、10/1-12/31: 205 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 30 件の報告があった。
[1/1-3/31: 13 件、4/1-6/30: 10 件、7/1-9/30: 1 件、10/1-12/31: 6 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 10,857 件の報告があった。

[1/1-3/31：1,753 件、4/1-6/30：1,947 件、7/1-9/30：3,457 件、10/1-12/31：3,700 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は報告がなかった。

[1/1-3/31：0 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 19 件の報告があった。

[1/1-3/31：6 件、4/1-6/30：1 件、7/1-9/30:6 件、10/1-12/31：6 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 2,430 件の報告があった。

[1/1-3/31：670 件、4/1-6/30：491 件、7/1-9/30：837 件、10/1-12/31：432 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]

2019 年 1 月	2019 年 1 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 2019 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 Adobe Acrobat および Reader の脆弱性（APSB19-02）に関する注意喚起
2019年2月	Drupal の脆弱性（CVE-2019-6340）に関する注意喚起 ISC BIND 9 に対する複数の脆弱性（CVE-2018-5744, CVE-2018-5745, CVE-2019-6465）に関する注意喚起 Adobe Acrobat および Reader の脆弱性（APSB19-13）に関する注意喚起 runc の権限昇格の脆弱性（CVE-2019-5736）に関する注意喚起 2019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 Adobe Flash Player の脆弱性（APSB19-06）に関する注意喚起 Adobe Acrobat および Reader の脆弱性（APSB19-07）に関する注意喚起
2019年3月	2019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 Adobe ColdFusion の脆弱性（APSB19-14）に関する注意喚起
2019年4月	Oracle WebLogic Server の脆弱性（CVE-2019-2725）に関する注意喚起 ISC BIND 9 に対する複数の脆弱性に関する注意喚起 Confluence Server および Confluence Data Center における複数の脆弱性に関する注意喚起 2019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 2019年 4月 Intel 製品の脆弱性に関する注意喚起 2019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 Adobe Flash Player の脆弱性（APSB19-19）に関する注意喚起 Adobe Acrobat および Reader の脆弱性（APSB19-17）に関する注意喚起
2019年5月	Intel 製品の複数の脆弱性（INTEL-SA-00213）に関する注意喚起 2019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 Acrobat および Reader の脆弱性（APSB19-18）に関する注意喚起 Adobe Flash Player の脆弱性（APSB19-26）に関する注意喚起

2019年6月	Oracle WebLogic Server の脆弱性（CVE-2019-2729）に関する注意喚起 Firefox の脆弱性（CVE-2019-11707）に関する注意喚起 2019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 Adobe Flash Player の脆弱性（APSB19-30）に関する注意喚起
2019年7月	2019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 2019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
2019年8月	2019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 Adobe Acrobat および Reader の脆弱性（APSB19-41）に関する注意喚起
2019年9月	Microsoft Internet Explorer の脆弱性（CVE-2019-1367）に関する注意喚起 2019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 Flash Player の脆弱性（APSB19-46）に関する注意喚起 ウイルスバスター コーポレートエディションの脆弱性（CVE-2019-9489）に関する注意喚起 複数の SSL VPN 製品の脆弱性に関する注意喚起
2019年10月	ウイルスバスターコーポレートエディションの脆弱性（CVE-2019-18187）に関する注意喚起 2019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 Adobe Acrobat および Reader の脆弱性（APSB19-49）に関する注意喚起 2019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
2019年11月	マルウエア Emotet の感染に関する注意喚起 ISC BIND 9 の脆弱性に関する注意喚起 2019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
2019年12月	2019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

	Adobe Acrobat および Reader の脆弱性（APSB19-55）に関する注意喚起 ISC BIND 9 の脆弱性に関する注意喚起

（２） 活動概要（報告状況等の公表）

発行日：2019-01-16［ 2018 年 10 月 1 日 ～ 2018 年 12 月 31 日］
発行日：2019-04-11［ 2019 年 1 月 1 日 ～ 2019 年 3 月 31 日］
発行日：2019-07-11［ 2019 年 4 月 1 日 ～ 2019 年 6 月 30 日］
発行日：2019-10-17［ 2019 年 7 月 1 日 ～ 2019 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］323 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。