不正アクセス行為の発生状況

第１　平成28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

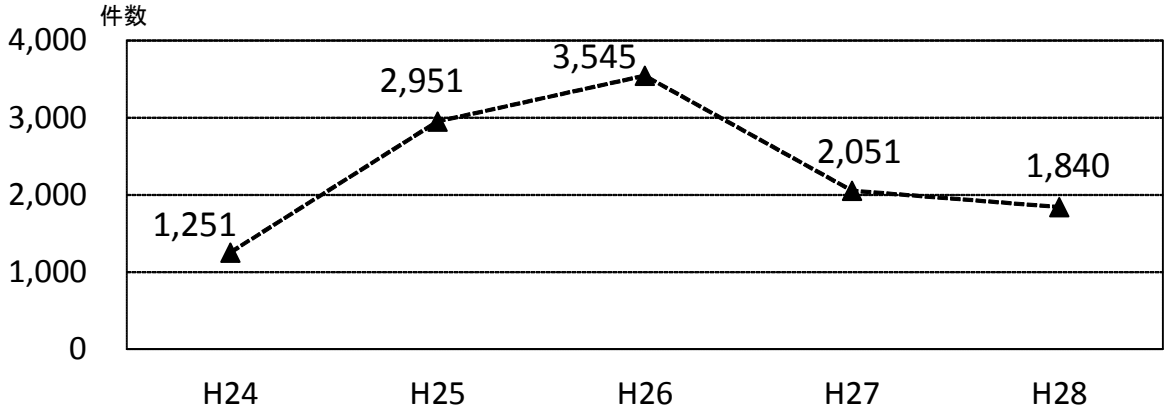
平成28年に都道府県警察から警察庁に報告のあった不正アクセス行為を対象とした。

１　不正アクセス行為の認知状況

(1)　認知件数

平成28年における不正アクセス行為の認知件数[注1]は1,840件であり、前年と比べ、211件減少した。

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]別に内訳をみると、「一般企業」が最も多く1,823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24年	平成25年	平成26年	平成27年	平成28年
一般企業	1,163	2,893	3,468	1,998	1,823
プロバイダ	22	9	16	11	6
行政機関等	52	24	3	14	5
大学、研究機関等	12	9	56	11	2
その他	2	16	2	17	4
計(件)	1,251	2,951	3,545	2,051	1,840

※「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。
※「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。
※「大学、研究機関等」には、高等学校等の教育機関を含む。

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みると、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が最も多く（828件）、次いで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（511件）、利用権者[注3]からの届出によるもの（495件）の順となっている。

図１－２　平成28年における認知の端緒別認知件数

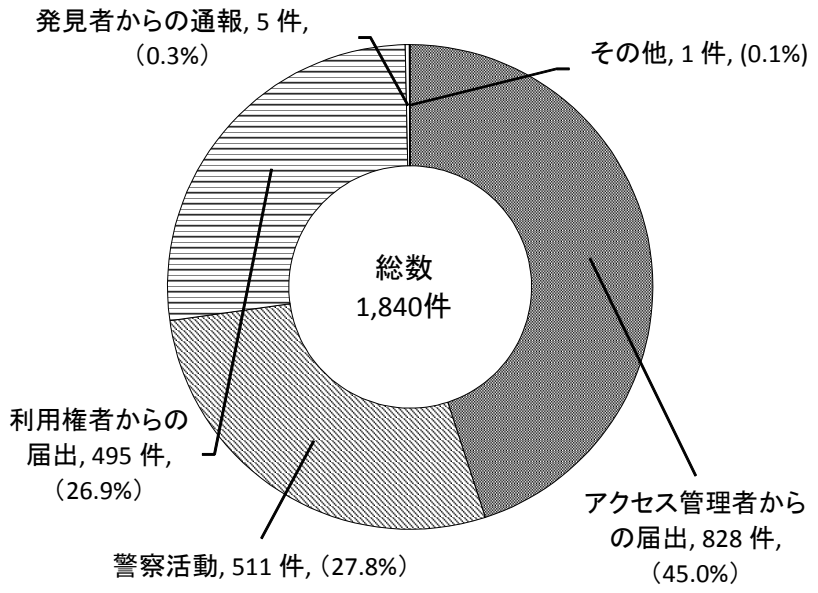


表１－２　過去５年の認知の端緒別認知件数

区分＼年次	平成24年	平成25年	平成26年	平成27年	平成28年
アクセス管理者からの届出	80	1,208	1,848	910	828
警察活動	270	781	119	516	511
利用権者からの届出	892	929	1,337	614	495
発見者からの通報	5	20	238	11	5
その他	4	13	3	0	1
計（件）	1,251	2,951	3,545	2,051	1,840

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みると、「インターネットバンキングでの不正送金」が最も多く（1,305件）、次いで「インターネットショッピングでの不正購入」（172件）、「オンラインゲーム、コミュニティサイトの不正操作」（124件）の順となっている。

図１－３　平成28年における不正アクセス後の行為別認知件数

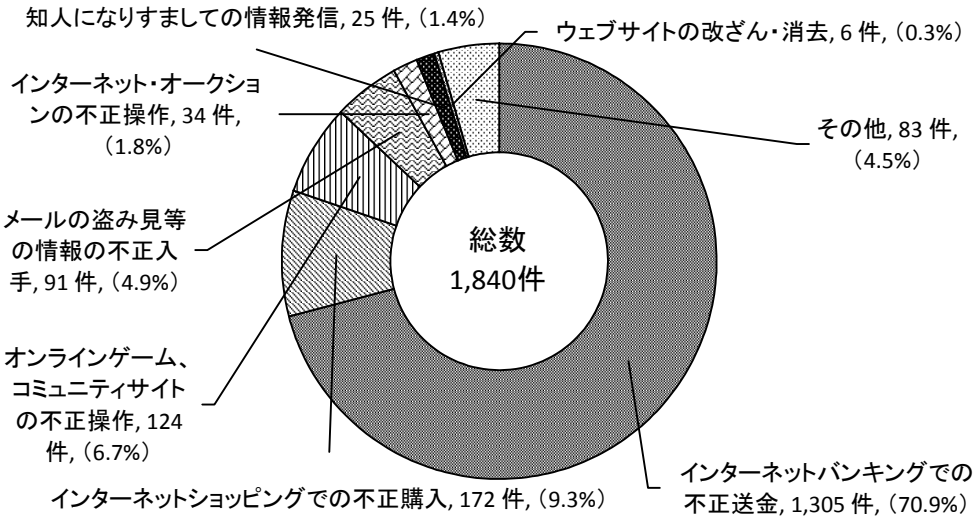


表１－３　過去５年の不正アクセス後の行為別認知件数

区分＼年次	平成24年	平成25年	平成26年	平成27年	平成28年
インターネットバンキングでの不正送金	95	1,325	1,944	1,531	1,305
インターネットショッピングでの不正購入	223	911	209	167	172
オンラインゲーム、コミュニティサイトの不正操作	662	379	130	96	124
メールの盗み見等の情報の不正入手	99	92	177	92	91
インターネット・オークションの不正操作	29	36	13	20	34
知人になりすましての情報発信	65	26	1,009	83	25
ウェブサイトの改ざん・消去	42	107	40	34	6
その他	36	75	23	28	83
計（件）	1,251	2,951	3,545	2,051	1,840

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28年における不正アクセス禁止法違反の検挙件数は502件、検挙人員は200人であり、前年と比べ、検挙件数は129件増加し、検挙人員は27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みると、「不正アクセス行為」が462件、192人、「識別符号の提供（助長）行為[注4]」が５件、３人、「識別符号の取得行為[注5]」が６件、３人、「識別符号の保管行為[注6]」が28件、６人、「フィッシング行為[注7]」が１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24年	平成25年	平成26年	平成27年	平成28年
不正アクセス行為	検挙件数	533	968	338	332	462
	検挙事件数[注8]	133	142	141	154	175
	検挙人員	151	144	150	154	192
識別符号提供（助長）行為	検挙件数	4	7	0	5	5
	検挙事件数	4	7	0	5	2
	検挙人員	4	7	0	5	3
識別符号取得行為	検挙件数	2	2	16	10	6
	検挙事件数	2	1	5	1	3
	検挙人員	2	1	15	1	3
識別符号保管行為	検挙件数	2	2	2	12	28
	検挙事件数	2	2	2	2	6
	検挙人員	2	2	2	2	6
フィッシング行為	検挙件数	2	1	8	14	1
	検挙事件数	1	1	6	14	1
	検挙人員	1	1	6	14	1
計	検挙件数（件）	543	980	364	373	502
	検挙事件数（事件）	136（重複6）	145（重複8）	150（重複4）	173（重複3）	182（重複5）
	検挙人員（人）	154（重複6）	147（重複8）	170（重複3）	173（重複3）	200（重複5）

※　１事件で複数の区分の行為を検挙した場合及び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　相手方に不正アクセスの目的があることを知りながら、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及び検挙事件数について手口別に内訳をみると、「識別符号窃用型[注9]」が457件、「セキュリティ・ホール攻撃型[注10]」が５件となっている。

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24年	平成25年	平成26年	平成27年	平成28年
識別符号窃用型	検挙件数	532	965	336	331	457
	検挙事件数	133	139	140	153	174
セキュリティ・ホール攻撃型	検挙件数	1	3	2	1	5
	検挙事件数	1	3	2	1	3
計	検挙件数（件）	533	968	338	332	462
	検挙事件数（事件）	133（重複1）	142	141（重複1）	154	175（重複2）

※　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。

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情報（他人の識別符号を入力する場合を除く。）や指令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２号又は第３号に該当する行為）をいう。例えば、セキュリティの脆弱性を突いて操作指令を与えるなどの手法による不正アクセス行為が該当する。

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

不正アクセス禁止法違反に係る被疑者の年齢は、「14～19歳」（62人）が最も多く、次いで「20～29歳」（56人）、「30～39歳」（48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63歳であった。

図３－１　平成28年における年代別被疑者数

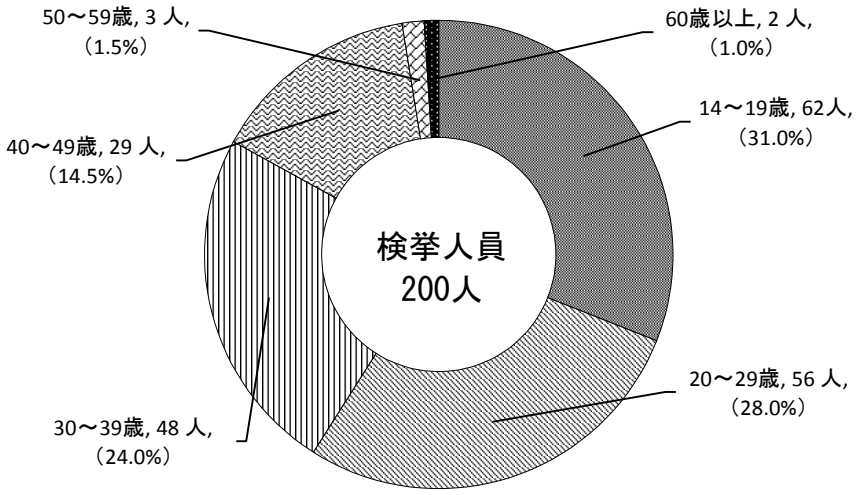


表３－１　過去５年の年代別被疑者数の推移

区分＼年次	平成24年	平成25年	平成26年	平成27年	平成28年
14～19歳	64	44	49	53	62
20～29歳	34	30	43	43	56
30～39歳	21	37	45	41	48
40～49歳	28	27	25	29	29
50～59歳	6	8	5	5	3
60歳以上	1	1	3	2	2
計（人）	154	147	170	173	200

(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（106人）、次いで「交友関係のない他人によるもの」（67人）、「ネットワーク上の知り合いによるもの」（27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５名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、検挙事件としては計上されない。

(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みると、「利用権者のパスワード設定・管理の甘さにつけ込んだもの」が最も多く（244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」（61件）、「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」（49件）の順となっている。

図３－２　平成28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

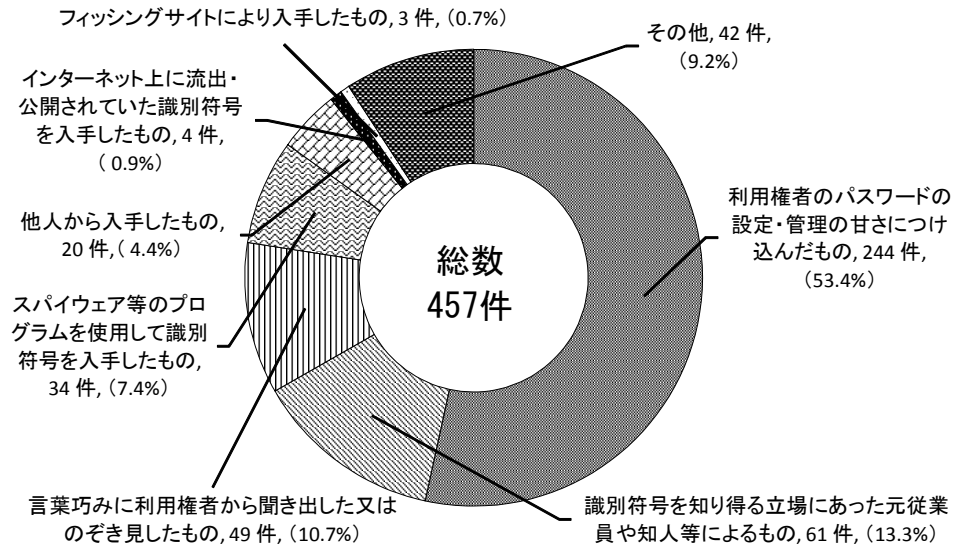


表３－２　過去５年の不正アクセス行為に係る手口別検挙件数

区分＼年次	平成24年	平成25年	平成26年	平成27年	平成28年
識別符号窃用型（件）	532	965	336	331	457
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	122	767	84	117	244
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	101	56	47	51	61
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	229	64	53	46	49
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	29	25	6	15	34
他人から入手したもの	16	33	25	13	20
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	6	9	34	57	4
フィッシングサイトにより入手したもの	18	9	71	24	3
その他	11	2	16	8	42
セキュリティ・ホール攻撃型（件）	1	3	2	1	5

注13　パソコン内のファイル情報、キーボードの入力情報又は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みると、「好奇心を満たすため」が最も多く（208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」（70件）、「嫌がらせや仕返しのため」（44件）の順となっている。

図３－３　平成28年における不正アクセス行為に係る動機別検挙件数

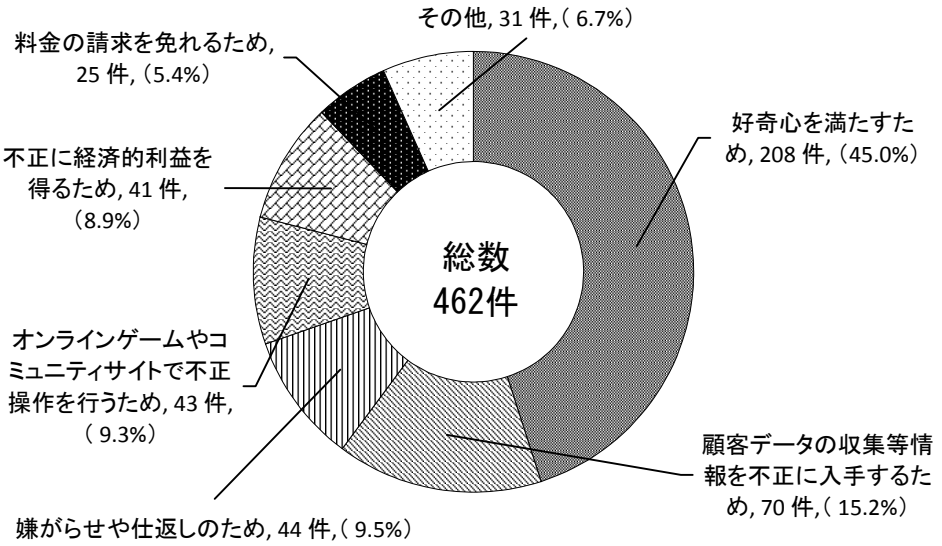


表３－３　過去５年の不正アクセス行為に係る動機別検挙件数

区分＼年次	平成24年	平成25年	平成26年	平成27年	平成28年
好奇心を満たすため	85	46	15	76	208
顧客データの収集等情報を不正に入手するため	38	53	139	72	70
嫌がらせや仕返しのため	100	56	54	44	44
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	219	77	41	28	43
不正に経済的利益を得るため	79	706	86	52	41
料金の請求を免れるため	10	25	2	58	25
その他	2	5	1	2	31
計（件）	533	968	338	332	462

(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（457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に内訳をみると、「オンラインゲーム、コミュニティサイト」が最も多く（185件）、次いで「電子メール」（136件）、「社員・会員用等の専門サイト」（40件）の順となっている。

図３－４　平成27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

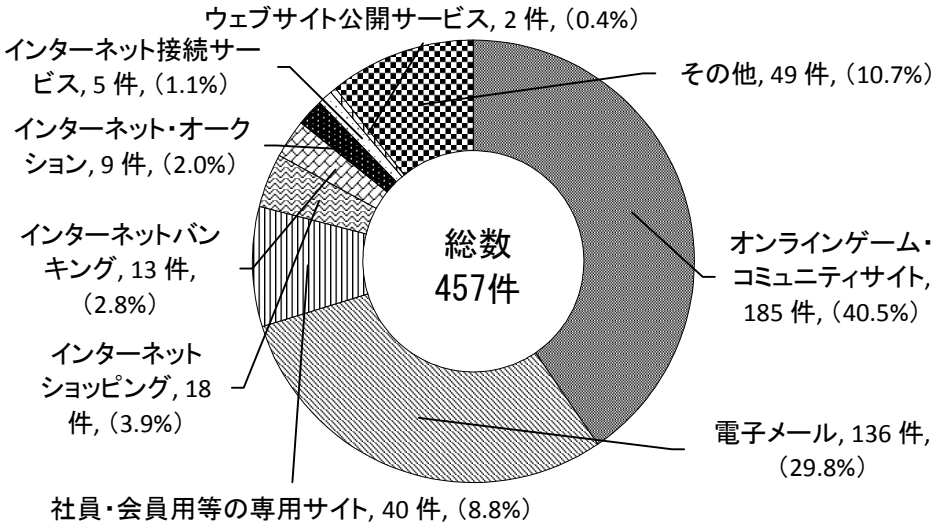


表３－４　過去５年の不正に利用されたサービス別検挙件数

区分＼年次	平成24年	平成25年	平成26年	平成27年	平成28年
識別符号窃用型　（件）	532	965	336	331	457
オンラインゲーム、コミュニティサイト	318	138	69	116	185
電子メール	44	48	30	64	136
社員・会員用等の専用サイト	98	15	65	20	40
インターネットショッピング	28	728	44	54	18
インターネットバンキング	31	7	20	30	13
インターネット・オークション	5	5	15	20	9
インターネット接続サービス	0	0	11	11	5
ウェブサイト公開サービス	8	6	7	9	2
その他	0	18	75	7	49

４　検挙事例

(1)　無職の少年（17）らは、平成28年１月から同年５月までの間、佐賀県教育情報システムに不正にアクセスし、職員、生徒及び保護者の個人情報、生徒の成績等約21万件のファイルを入手した。同年６月、不正アクセス禁止法違反（不正アクセス行為）等で逮捕した（警視庁・佐賀）。

(2)　県職員の男（46）は、ＳＮＳサイト、情報検索サイト等のアカウントに氏名と生年月日を組み合わせたものを使用している利用権者が多いことを利用してＩＤ・パスワードを類推し、平成26年９月から平成27年６月までの間、女性芸能人のアカウントに繰り返し不正にアクセスし、個人情報、私的な画像、メール等を入手した。平成28年１月、不正アクセス禁止法違反（不正アクセス行為）で逮捕した（神奈川）。

(3)　高校生の少年（16）らは、平成27年５月から同年11月までの間、ＳＱＬインジェクション[注14]による不正アクセスにより、企業のサーバコンピュータから多数の他人のＩＤ・パスワードを不正に取得し、同年８月から同年11月までの間、同ＩＤ・パスワードを使用してショッピングサイトに不正にアクセスして玩具を購入した。平成28年９月、不正アクセス禁止法違反（不正アクセス行為）等で送致した（宮城）。

(4)　無職の男（34）らは、平成27年１月、他人のＩＤ・パスワードをだまし取るため、オークションサイトを模した、いわゆる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利用者にＩＤ・パスワードを入力させてこれを詐取した上、同ＩＤ・パスワードを使用して正規オークションサイトに不正にアクセスし、オークションに架空の出品を行い、代金をだまし取るなどした。平成28年11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）等で逮捕した（神奈川）。

(5)　会社員の男（28）は、平成28年２月、ＳＮＳサイト上で知り合った女子高校生のＩＤ・パスワードを類推して不正にアクセスし、パスワード等を書き換えるなどしてアカウントを乗っ取った。同年11月、不正アクセス禁止法違反（不正アクセス行為）等で逮捕した（香川）。

注14　ＳＱＬというプログラム言語を用いて、企業等が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。

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

平成28年における不正アクセス行為（識別符号窃用型）の手口のうち、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半数以上を占めていることから、パスワードを設定する場合には、ＩＤと全く同じパスワードやＩＤの一部を使ったパスワード等、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、パスワードを定期的に変更するなど、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、発信元に心当たりのない電子メール等には注意する。また、金融機関等が電子メールで口座番号や暗証番号等の個人情報を問い合わせることはなく、これらの入力を求める電子メールは、金融機関等を装ったフィッシングメールであると考えられるため、個人情報は入力しない。

(3)　不正プログラムに対する注意

コンピュータに不正プログラムを感染させ、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、心当たりのない企業からの請求書をかたった電子メール等に添付されたファイルは不用意に開かず、信頼できないウェブサイト上に蔵置されたファイルはダウンロードしない。また、不特定多数が利用するコンピュータでは重要な情報を入力しない。さらに、コンピュータ・ウイルス等の不正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に係る不正送金事犯では、原因の多くが不正プログラムの感染によるものと認められることから、セキュリティ対策ソフトやワンタイムパスワード[注15]、二経路認証[注16]の導入等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　アクセス管理者等の講ずべき措置

(1)　フィッシングや不正プログラム等への対策

フィッシングや不正プログラム等により取得した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、フィッシングや不正プログラム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、インターネットショッピング、オンラインゲーム、インターネットバンキング等のサービスを提供する事業者は、ワンタイムパスワード、二経路認証の導入等により個人認証を強化するなどの対策を講ずる。

注15　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16　インターネットバンキングにおいて、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。

(2)　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、アクセス管理者は、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、複数のサイトで同じパスワードを使用することの危険性を周知する、定期的にパスワードの変更を促す仕組みを構築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。

(3)　ＩＤ・パスワードの適切な管理

ＩＤ・パスワードを知り得る立場にあった元従業員による不正アクセス行為が発生していることから、従業員が退職したときや特定電子計算機を利用する立場でなくなったときには、当該従業員に割り当てていた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)　セキュリティ・ホール攻撃への対応

セキュリティ・ホール攻撃の一つであるＳＱＬインジェクション攻撃によって個人情報が流出する事案や、ウェブサーバの脆弱性に対する攻撃によってウェブサイトが改ざんされる事案への対策として、アクセス管理者は、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等を導入し、セキュリティ・ホール攻撃に対する監視体制を強化する。

（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28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83件（平成27年：110件）であった。（注２）

平成28年は同27年と比べて、27件（約24.5%）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87件（平成27年：160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40件（平成27年：118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。

17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。

６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５件である。

【主な内容】

パスワード推測：４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17件の届出があった。

【主な内容】

ファイル等の改ざん、破壊等：８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：７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、７件（平成27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、40件（平成27年：31件）の届出があった。

【主な内容】

正規ユーザへのなりすまし：31件

メール不正中継：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。

83件の届出中、実際に被害に遭った計61件（平成27年：88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：26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：６件

原因不明：15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：16 件

メールサーバ：９件

DNS サーバ：５件

不明：32 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

83 件の届出を被害内容で分類した 90 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 54 件（平成 27 年： 116 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】

オンラインサービスの不正利用：17 件

踏み台として悪用：13 件

ホームページ改ざん：９件

サービス低下：７件

データの窃取や盗み見：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 28 年では、芸能人のＳＮＳアカウントの不正ログイン被害など、パスワードの使い回しや推測が容易なパスワード設定が原因と思われる不正ログイン被害の報道が散見された。実際、不正アクセス届出においても被害に遭った 61 件のうち「ID、パスワード管理の不備」が原因とされる届出が 26 件（約 42.6%）と、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
http://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）
http://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 28 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 16,446 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 14,857 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 6,449 件の報告があった。

[1/1-3/31:1,654 件、4/1-6/30:1,520 件、7/1-9/30:1,098 件、10/1-12/31: 2,177 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 3,575 件の報告があった。

[1/1-3/31: 1,268 件、4/1-6/30: 1,065 件、7/1-9/30: 554 件、10/1-12/31: 688 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 994 件の報告があった。

[1/1-3/31: 100 件、4/1-6/30: 181 件、7/1-9/30: 337 件、10/1-12/31: 376 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 212 件の報告があった。

[1/1-3/31: 86 件、4/1-6/30: 11 件、7/1-9/30: 54 件、10/1-12/31: 61 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 2,275 件の報告があった。

[1/1-3/31: 645 件、4/1-6/30: 642 件、7/1-9/30: 467 件、10/1-12/31: 521 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 55 件の報告があった。

[1/1-3/31: 11 件、4/1-6/30: 15 件、7/1-9/30: 5 件、10/1-12/31: 24 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 46 件の報告があった。

[1/1-3/31: 6 件、4/1-6/30: 15 件、7/1-9/30: 10 件、10/1-12/31: 15 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 1,251 件の報告があった。

[1/1-3/31: 373 件、4/1-6/30: 342 件、7/1-9/30: 276 件、10/1-12/31: 260 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]

2016 年 1 月	Adobe Flash Player の脆弱性 (APSB16-01) に関する注意喚起 DNS ゾーン転送の設定不備による情報流出の危険性に関する注意喚起

	Adobe Reader および Acrobat の脆弱性（APSB16-02）に関する注意喚起 2016年1月 Microsoft セキュリティ情報（緊急 6件含）に関する注意喚起 2016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 ISC BIND 9 サービス運用妨害の脆弱性（CVE-2015-8704）に関する注意喚起
2016年2月	2016年2月 Microsoft セキュリティ情報（緊急 6件含）に関する注意喚起 Adobe Flash Player の脆弱性（APSB16-04）に関する注意喚起 glibc ライブラリの脆弱性（CVE-2015-7547）に関する注意喚起
2016年3月	OpenSSL の複数の脆弱性に関する注意喚起 2016年3月 Microsoft セキュリティ情報（緊急 5件含）に関する注意喚起 Adobe Reader および Acrobat の脆弱性（APSB16-09）に関する注意喚起 ISC BIND 9 サービス運用妨害の脆弱性（CVE-2016-1286）に関する注意喚起 Adobe Flash Player の脆弱性（APSB16-08）に関する注意喚起 Oracle Java SE の脆弱性（CVE-2016-0636）に関する注意喚起
2016年4月	Adobe Flash Player の脆弱性（APSB16-10）に関する注意喚起 2016年4月 Microsoft セキュリティ情報（緊急 6件含）に関する注意喚起 2016年4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 ケータイキット for Movable Type の脆弱性（CVE-2016-1204）に関する注意喚起 Apache Struts 2 の脆弱性（S2-032）に関する注意喚起
2016年5月	ImageMagick の脆弱性（CVE-2016-3714）に関する注意喚起 2016 年 5 月 Microsoft セキュリティ情報（緊急 8 件含）に関する注意喚起 Adobe Reader および Acrobat の脆弱性（APSB16-14）に関する注意喚起 Adobe Flash Player の脆弱性（APSB16-15）に関する注意喚起
2016年6月	2016 年 6 月 Microsoft セキュリティ情報（緊急 5 件含）に関す

	る注意喚起 Adobe Flash Player の脆弱性（APSB16-18）に関する注意喚起 Apache Struts 2 の脆弱性（S2-037）に関する注意喚起
2016 年 7 月	2016 年 7 月 Microsoft セキュリティ情報（緊急 6 件含）に関する注意喚起 Adobe Flash Player の脆弱性（APSB16-25）に関する注意喚起 Adobe Reader および Acrobat の脆弱性（APSB16-26）に関する注意喚起 CGI 等を利用する Web サーバの脆弱性（CVE-2016-5385 等）に関する注意喚起 2016 年 7 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
2016 年 8 月	2016 年 8 月 Microsoft セキュリティ情報（緊急 5 件含）に関する注意喚起
2016 年 9 月	Adobe Flash Player の脆弱性（APSB16-29）に関する注意喚起 2016 年 9 月 Microsoft セキュリティ情報（緊急 7 件含）に関する注意喚起 Web サイトで使用されるソフトウエアの脆弱性を悪用した攻撃に関する注意喚起 ISC BIND 9 サービス運用妨害の脆弱性（CVE-2016-2776）に関する注意喚起 OpenSSL の脆弱性（CVE-2016-6309）に関する注意喚起
2016 年 10 月	2016 年 10 月 Microsoft セキュリティ情報（緊急 5 件含）に関する注意喚起 Adobe Flash Player の脆弱性（APSB16-32）に関する注意喚起 Adobe Reader および Acrobat の脆弱性（APSB16-33）に関する注意喚起 2016 年 10 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 Adobe Flash Player の脆弱性（APSB16-36）に関する注意喚起
2016 年 11 月	ISC BIND 9 サービス運用妨害の脆弱性（CVE-2016-8864）に関する注意喚起 Adobe Flash Player の脆弱性（APSB16-37）に関する注意喚起 2016 年 11 月 Microsoft セキュリティ情報（緊急 6 件含）に関する注意喚起 Web サイト改ざんに関する注意喚起

2016 年 12 月	Adobe Flash Player の脆弱性（APSB16-39）に関する注意喚起 2016 年 12 月 Microsoft セキュリティ情報（緊急 6 件含）に関する注意喚起 インターネットに接続された機器の管理に関する注意喚起 SKYSEA Client View の脆弱性（CVE-2016-7836）に関する注意喚起

（２） 活動概要（報告状況等の公表）

発行日：2017-01-11［ 2016 年 10 月 1 日～ 2016 年 12 月 31 日］
発行日：2016-10-12［ 2016 年 7 月 1 日 ～ 2016 年 9 月 30 日］
発行日：2016-07-14［ 2016 年 4 月 1 日 ～ 2016 年 6 月 30 日］
発行日：2016-04-14［ 2016 年 1 月 1 日 ～ 2016 年 3 月 31 日］

（３） JPCERT/CC レポート

［発行件数］51 件
［取り扱ったセキュリティ関連情報数］377 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。