

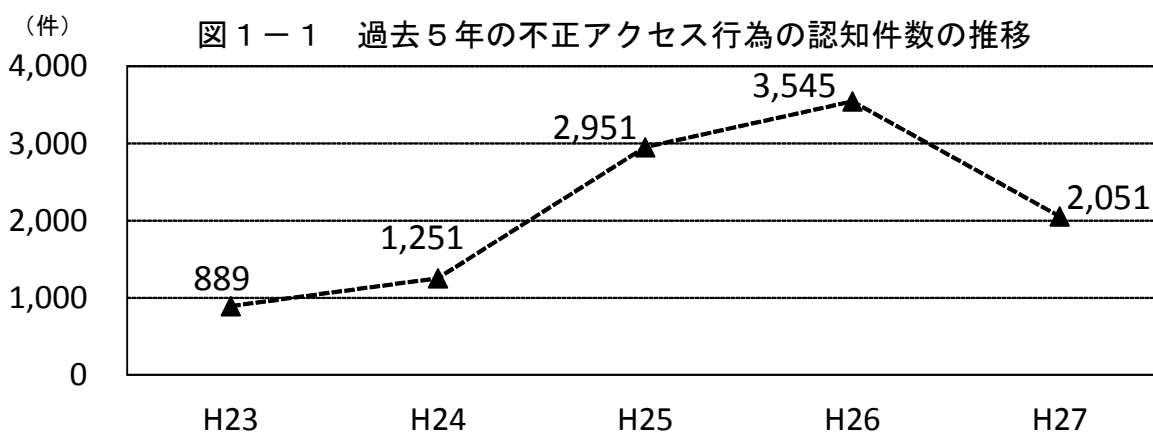
不正アクセス行為の発生状況

第1 平成27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27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27年における不正アクセス行為の認知件数^{注1}は2,051件であり、前年と比べ、1,494件減少した。



(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1,998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23年	平成24年	平成25年	平成26年	平成27年
一般企業		762	1,163	2,893	3,468	1,998
行政機関等		6	52	24	3	14
プロバイダ		115	22	9	16	11
大学、研究機関等		1	12	9	56	11
その他		5	2	16	2	17
計(件)		889	1,251	2,951	3,545	2,051

※「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。

※「大学、研究機関等」には、高等学校等の教育機関を含む。

注1 ここでの認知件数とは、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（910件）、次いで利用権者^{注3}からの届出によるもの（614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（516件）の順となっている。

図 1 - 2 平成27年における認知の端緒別認知件数

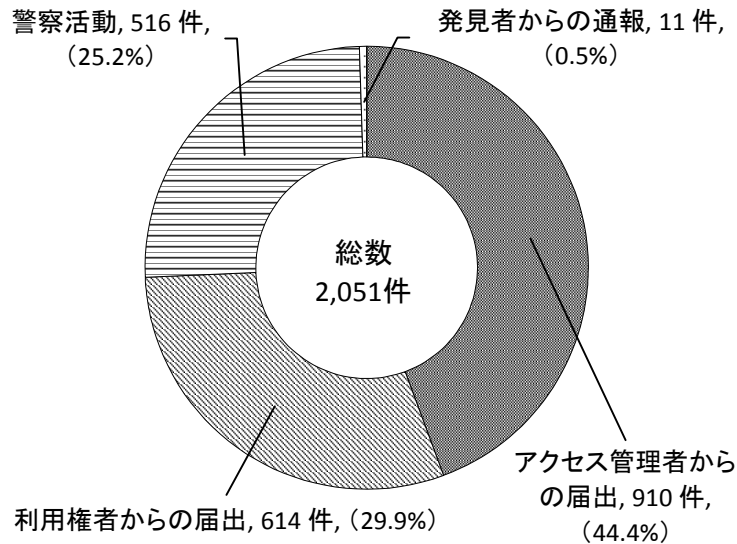


表 1 - 2 過去5年の認知の端緒別認知件数

区分 \ 年次	平成23年	平成24年	平成25年	平成26年	平成27年
アクセス管理者からの届出	121	80	1,208	1,848	910
利用権者からの届出	680	892	929	1,337	614
警察活動	75	270	781	119	516
発見者からの通報	7	5	20	238	11
その他	6	4	13	3	0
計 (件)	889	1,251	2,951	3,545	2,051

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（1,531件）、次いで「インターネットショッピングでの不正購入」（167件）、「オンラインゲーム、コミュニティサイトの不正操作」（96件）、「メールの盗み見等の情報の不正入手」（92件）の順となっている。

図 1-3 平成27年における不正アクセス後の行為別認知件数

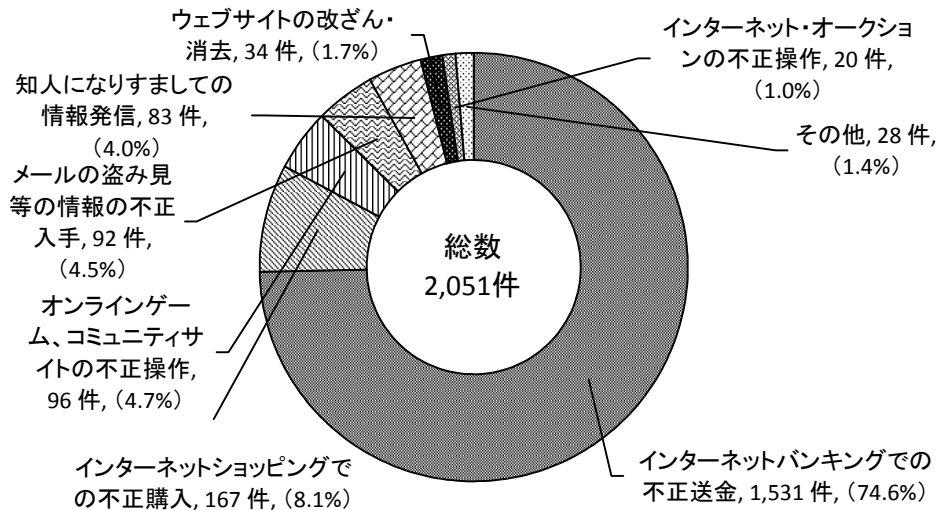


表 1-3 過去5年の不正アクセス後の行為別認知件数

区分	年次				
	平成23年	平成24年	平成25年	平成26年	平成27年
インターネットバンキングでの不正送金	188	95	1,325	1,944	1,531
インターネットショッピングでの不正購入	172	223	911	209	167
オンラインゲーム、コミュニティサイトの不正操作	358	662	379	130	96
メールの盗み見等の情報の不正入手	74	99	92	177	92
知人になりすましての情報発信	18	65	26	1,009	83
ウェブサイトの改ざん・消去	28	42	107	40	34
インターネット・オークションの不正操作	22	29	36	13	20
その他	29	36	75	23	28
計（件）	889	1,251	2,951	3,545	2,051

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27年における不正アクセス禁止法違反の検挙件数は373件、検挙人員は173人であり、前年と比べ、検挙件数は9件増加し、検挙人員は3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332件、154人、「識別符号の提供（助長）行為^{注4}」が5件、5人「識別符号の取得行為^{注5}」が10件、1人、「識別符号の保管行為^{注6}」が12件、2人、「フィッシング行為^{注7}」が14件、14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23年	平成24年	平成25年	平成26年	平成27年
不正アクセス行為	検挙件数	242	533	968	338	332
	検挙事件数 ^{注8}	101	133	142	141	154
	検挙人員	110	151	144	150	154
識別符号提供（助長）行為	検挙件数	6	4	7	0	5
	検挙事件数	6	4	7	0	5
	検挙人員	6	4	7	0	5
識別符号取得行為	検挙件数		2	2	16	10
	検挙事件数		2	1	5	1
	検挙人員		2	1	15	1
識別符号保管行為	検挙件数		2	2	2	12
	検挙事件数		2	2	2	2
	検挙人員		2	2	2	2
フィッシング行為	検挙件数		2	1	8	14
	検挙事件数		1	1	6	14
	検挙人員		1	1	6	14
計	検挙件数（件）	248	543	980	364	373
	検挙事件数（事件） （重複4）	103 （重複4）	136 （重複6）	145 （重複8）	150 （重複4）	173 （重複3）
	検挙人員（人） （重複2）	114 （重複2）	154 （重複6）	147 （重複8）	170 （重複3）	173 （重複3）

※ 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。

※ 識別符号取得行為、識別符号保管行為及びフィッシング行為は、平成24年の不正アクセス禁止法改正により新設された罪のため、平成24年からの計上となる。

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。

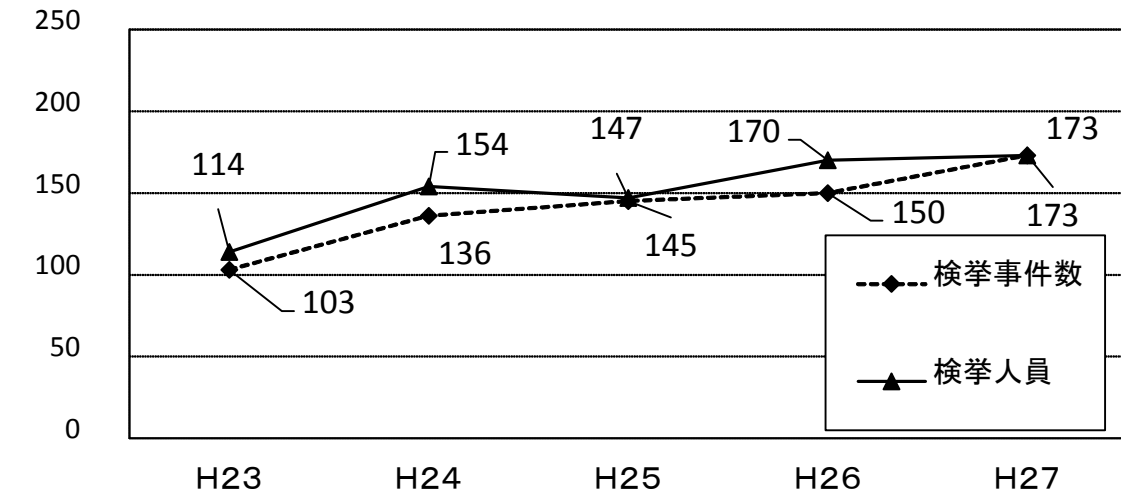
注5 不正アクセスの目的で他人の識別符号を取得する行為をいう。

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。

図 2 - 1 過去 5 年の検挙事件数及び検挙人員の推移



(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331件、「セキュリティ・ホール攻撃型^{注10}」が1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23年	平成24年	平成25年	平成26年	平成27年
識別符号窃用型	検挙件数	241	532	965	336	331
	検挙事件数	100	133	139	140	153
セキュリティ・ホール攻撃型	検挙件数	1	1	3	2	1
	検挙事件数	1	1	3	2	1
計	検挙件数 (件)	242	533	968	338	332
	検挙事件数 (事件)	101	133 (重複1)	142	141 (重複1)	154

※ 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」(53人)が最も多く、次いで「20～29歳」(43人)、「30～39歳」(41人)、「40～49歳」(29人)、「50～59歳」(5人)、「60歳以上」(2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72歳であった。

図3-1 平成27年における年代別被疑者数

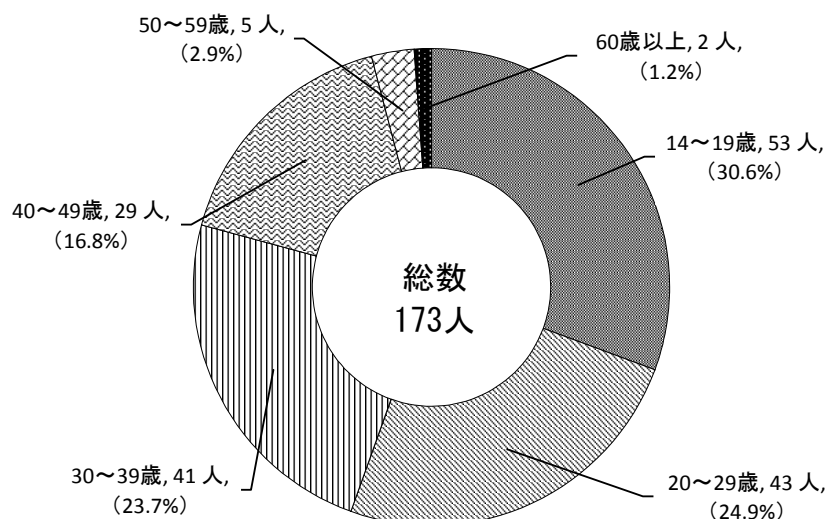


表3-1 過去5年の年代別被疑者数の推移

区分	年次	平成23年	平成24年	平成25年	平成26年	平成27年
14～19歳		51	64	44	49	53
20～29歳		30	34	30	43	43
30～39歳		19	21	37	45	41
40～49歳		10	28	27	25	29
50～59歳		2	6	8	5	5
60歳以上		2	1	1	3	2
計(人)		114	154	147	170	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見ると、「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(82人)、次いで「交友関係のない他人によるもの」(73人)、「ネットワーク上の知り合いによるもの」(18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8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（117件）、次いで「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件）、「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件）の順となっている。

図3-2 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

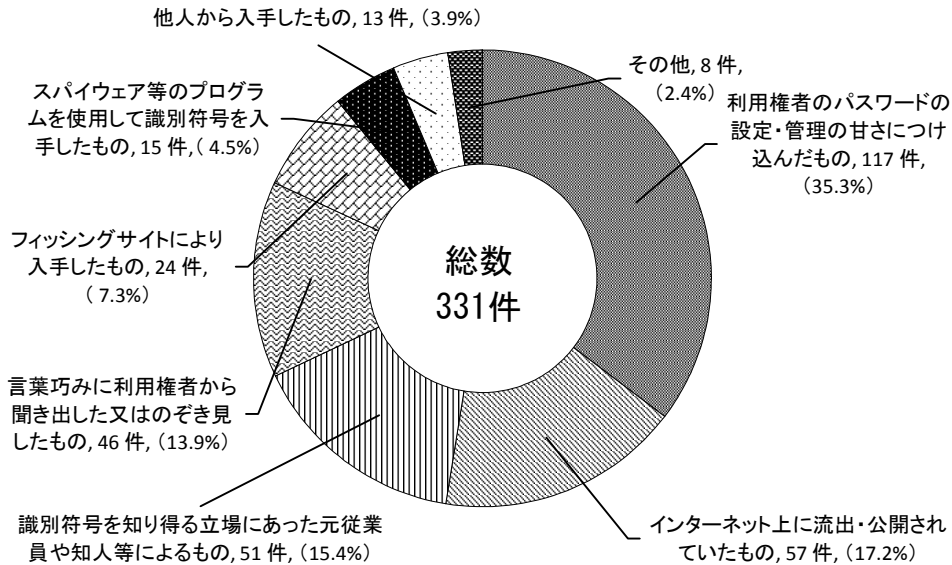


表3-2 過去5年の不正アクセス行為に係る手口別検挙件数

区分	年次				
	平成23年	平成24年	平成25年	平成26年	平成27年
識別符号窃用型（件）	241	532	965	336	331
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	59	122	767	84	117
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	1	6	9	34	57
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	52	101	56	47	51
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	29	229	64	53	46
フィッシングサイトにより入手したもの	59	18	9	71	24
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	1	29	25	6	15
他人から入手したもの	37	16	33	25	13
その他	3	11	2	16	8
セキュリティ・ホール攻撃型（件）	1	1	3	2	1

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（76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」（72件）、「料金の請求を免れるため」（58件）、「不正に経済的利益を得るため」（52件）の順となっている。

図3-3 平成27年における不正アクセス行為に係る動機別検挙件数

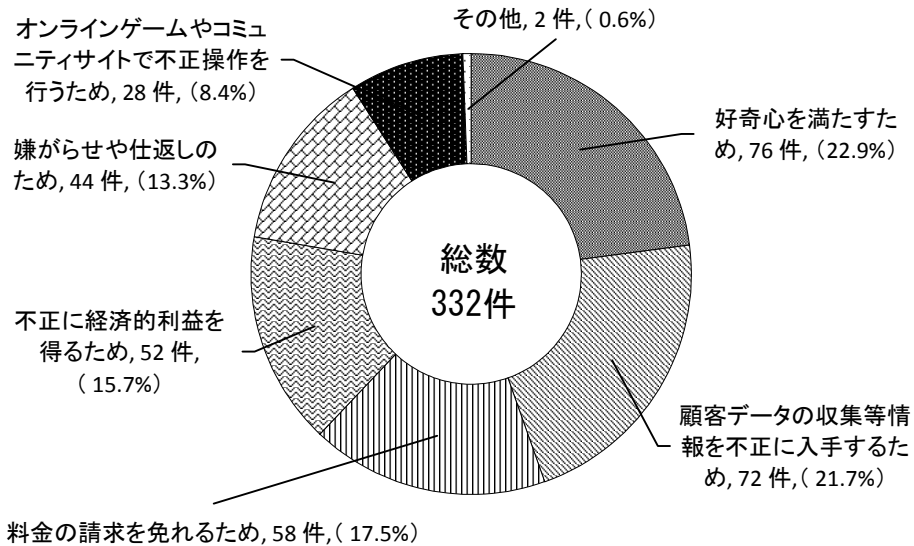


表3-3 過去5年の不正アクセス行為に係る動機別検挙件数

区分	年次	平成23年	平成24年	平成25年	平成26年	平成27年
	好奇心を満たすため	32	85	46	15	76
顧客データの収集等情報を不正に入手するため	15	38	53	139	72	
料金の請求を免れるため	0	10	25	2	58	
不正に経済的利益を得るため	97	79	706	86	52	
嫌がらせや仕返しのため	58	100	56	54	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	39	219	77	41	28	
その他	1	2	5	1	2	
計（件）		242	533	968	338	332

(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（331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（116件）、次いで「電子メール」（64件）、「インターネットショッピング」（54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

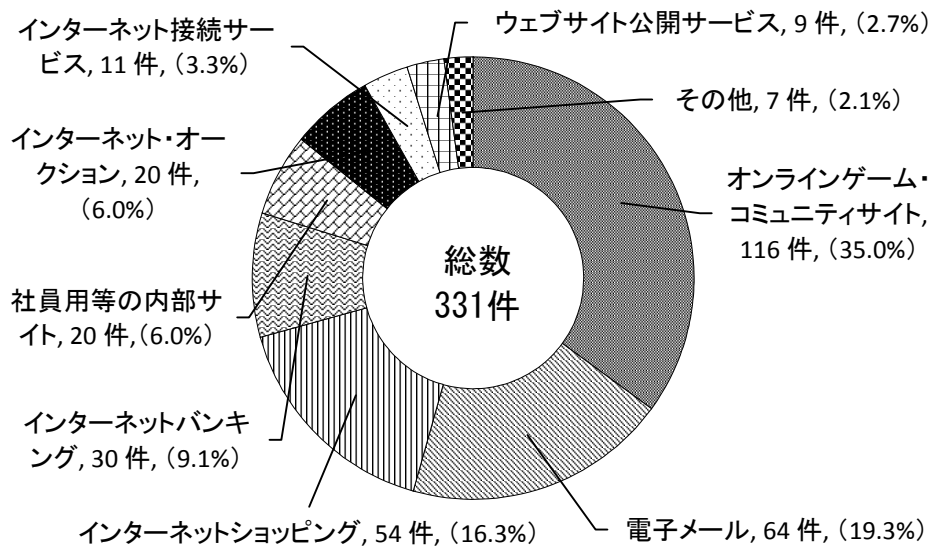


表3-4 過去5年の不正に利用されたサービス別検挙件数

区分	年次				
	平成23年	平成24年	平成25年	平成26年	平成27年
識別符号窃用型（件）	241	532	965	336	331
オンラインゲーム、コミュニティサイト	83	318	138	69	116
電子メール	23	44	48	30	64
インターネットショッピング	87	28	728	44	54
インターネットバンキング	14	31	7	20	30
社員用等の内部サイト	16	98	15	65	20
インターネット・オークション	4	5	5	15	20
インターネット接続サービス	0	0	0	11	11
ウェブサイト公開サービス	5	8	6	7	9
その他	9	0	18	75	7

4 都道府県公安委員会に対する援助の要請

平成27年中、不正アクセス禁止法第9条の規定に基づく、都道府県公安委員会に対する援助を受けたい旨の申出はなかった。

表4-1 過去5年の都道府県公安委員会に対する援助措置の要請件数

区分 \ 年次	平成23年	平成24年	平成25年	平成26年	平成27年
要請件数(件)	0	0	0	0	0

5 検挙事例

- (1) 中継サーバ事業を営む会社役員の男(39)らは、27年6月、他人の識別符号を用いてインターネットサービスプロバイダのサーバに不正にアクセスし、海外の顧客に対して国内プロバイダのインターネットサービスを利用させていた。同年11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(警視庁ほか)。
- (2) 無職の少年(19)は、27年2月、インターネット上に流出していた他人の識別符号を用いてインターネットサイトの会員向けサービスのサーバに不正にアクセスし、メールアドレス等のサーバ内に保存されている当該他人の登録情報を変更し、オークションサイトで商品を不正に入手していた。同年10月、不正アクセス禁止法違反(不正アクセス行為)及び私電磁的記録不正作出・同供用で逮捕した(神奈川)。
- (3) 無職の少年(17)は、26年12月、匿名化工作を行いながら、他人の識別符号を用いてレンタルサーバ会社が管理するサーバに不正にアクセスし、サーバ内に保存されている当該他人の登録パスワードを変更した。27年6月、不正アクセス禁止法違反(不正アクセス行為)及び私電磁的記録不正作出・同供用で逮捕した(警視庁)。
- (4) 元ホテル従業員である団体職員の男(37)は、26年10月、以前勤務していたホテルの識別符号を用いて大手旅行会社の宿泊予約サイトのサーバに不正にアクセスし、サーバ内に保存されている当該ホテルの客室情報を改ざんし予約済みの部屋を空室にするなどした。27年2月、不正アクセス禁止法違反(不正アクセス行為)及び私電磁的記録不正作出・同供用で逮捕した(滋賀)。
- (5) 会社員の男(38)は、27年4月から同年5月までの間、元交際相手の識別符号を用いてインターネットサイトの会員向けサービスのサーバに不正にアクセスし、メールをのぞき見ていた。同年6月、不正アクセス禁止法(不正アクセス行為)で逮捕した(愛知)。

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の甘さにつけ込んだ不正アクセス行為、知人等による不正アクセス行為、言葉巧みに聞き出したID・パスワードによる不正アクセス行為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パスワード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と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、信頼できない電子メール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14}の利用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の使用等により個人認証を強化するなどの対策を講ずる。

(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。

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。

(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^{注15}によって個人情報流出する事案や、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。

注15 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27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110件（平成26年：120件）であった。（注2）

平成27年は同26年と比べて、10件（約8.3%）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160件（平成26年：192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118件（平成26年：126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。

61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12件である。

【主な内容】

ソフトウェアのぜい弱性やバグを利用した攻撃：3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53件の届出があった。

【主な内容】

ファイル等の改ざん、破壊等：27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：16件

資源利用（ファイル、CPU使用）：4件

裏口（バックドア）の作成：2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ある。11件（平成26年：23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、31件（平成26年：43件）の届出があった。

【主な内容】

正規ユーザへのなりすまし：24件

ソーシャルエンジニアリング：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。

110件の届出中、実際に被害に遭った計88件（平成26年：102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：35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：15件

DoS攻撃：11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：6件
原因不明：16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：17件
DNS サーバ：4件
FTP サーバ：3件
不明：18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

110件の届出を被害内容で分類した138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116件（昨年：133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：33件
オンラインサービスの不正利用：16件
ホームページ改ざん：14件
サービス低下：13件
データの窃取や盗み見：12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

報道された情報によるとパスワードリスト攻撃が原因と考えられる不正ログイン被害が、2013年、2014年は目立っていたが、2015年には収束の兆しが見られている。

ただし、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は多く、「ID、パスワード管理の不備」が原因とされる届出が35件と、2014年の17件と比べて倍化している。ウェブサイト改ざん被害のようにサーバの脆弱性が起因するものではなく、サーバの脆弱性を解消

していても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

- ・ 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】

「脆弱性対策のチェックポイント」

https://www.ipa.go.jp/security/vuln/20050623_websecurity.html

「安全なウェブサイトの作り方 改訂第6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>

「Microsoft セキュリティセンター」(日本マイクロソフト社)

<http://www.microsoft.com/ja-jp/security/default.aspx>

「MyJVN」(セキュリティ設定チェック、バージョンチェック)

<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 27 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 19,624 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 16,590 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 8,933 件の報告があった。
[1/1-3/31: 2,980 件、4/1-6/30: 2,442 件、7/1-9/30: 1,985 件、10/1-12/31: 1,526 件]

（2） Web サイト改ざん

攻撃者もしくはマルウェアによって、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 2,859 件の報告があった。
[1/1-3/31: 792 件、4/1-6/30: 649 件、7/1-9/30: 592 件、10/1-12/31: 826 件]

（3） マルウェアサイト

閲覧することで PC がマルウェ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ェアを公開しているサイトについて 660 件の報告があった。
[1/1-3/31: 260 件、4/1-6/30: 197 件、7/1-9/30: 119 件、10/1-12/31: 84 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 135 件の報告があった。
[1/1-3/31: 32 件、4/1-6/30: 71 件、7/1-9/30: 21 件、10/1-12/31: 11 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 1,953 件の報告があった。

[1/1-3/31: 466 件、4/1-6/30: 491 件、7/1-9/30: 522 件、10/1-12/31: 474 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 21 件の報告があった。

[1/1-3/31: 5 件、4/1-6/30: 4 件、7/1-9/30: 0 件、10/1-12/31: 12 件]

(7) 標的型攻撃

特定の組織、企業、業種などを標的として、マルウェア感染や情報の窃取などを試みる攻撃について 131 件の報告があった。

[1/1-3/31:-件、4/1-6/30:60 件、7/1-9/30:59 件、10/1-12/31:12 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 1,898 件の報告があった。

[1/1-3/31: 950 件、4/1-6/30: 274 件、7/1-9/30: 450 件、10/1-12/31: 224 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.jpccert.or.jp/>参照。)

(1) 注意喚起

[新規]

2015 年 1 月	2015 年 1 月 Microsoft セキュリティ情報 (緊急 1 件含) に関する注意喚起 Adobe Flash Player の脆弱性 (APSB15-01) に関する注意
------------	--

	<p>喚起</p> <p>2015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</p> <p>Adobe Flash Player の脆弱性 (APSB15-03) に関する注意喚起</p>
2015年2月	<p>Adobe Flash Player の脆弱性 (APSB15-04) に関する注意喚起</p> <p>2015年2月 Microsoft セキュリティ情報 (緊急 3件含) に関する注意喚起</p>
2015年3月	<p>2015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</p> <p>Adobe Flash Player の脆弱性 (APSB15-05) に関する注意喚起</p>
2015年4月	<p>2015年4月 Microsoft セキュリティ情報 (緊急 4件含) に関する注意喚起</p> <p>2015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</p> <p>Adobe Flash Player の脆弱性 (APSB15-06) に関する注意喚起</p>
2015年5月	<p>2015年5月 Microsoft セキュリティ情報 (緊急 3件含) に関する注意喚起</p> <p>Adobe Flash Player の脆弱性 (APSB15-09) に関する注意喚起</p> <p>Adobe Reader および Acrobat の脆弱性 (APSB15-10) に関する注意喚起</p> <p>ランサムウェア感染に関する注意喚起</p>
2015年6月	<p>2015年6月 Microsoft セキュリティ情報 (緊急 2件含) に関する注意喚起</p> <p>Adobe Flash Player の脆弱性 (APSB15-11) に関する注意喚起</p> <p>Adobe Flash Player の脆弱性 (APSB15-14) に関する注意喚起</p>
2015年7月	<p>Adobe Flash Player の脆弱性 (APSB15-16) に関する注意喚起</p> <p>2015年7月 Adobe Flash Player の未修正の脆弱性に関する注意喚起</p> <p>Cisco 社製セキュリティアプライアンスソフトウェアの脆弱性に関する注意喚起</p> <p>2015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</p> <p>Adobe Reader および Acrobat の脆弱性 (APSB15-15) に関する注意喚起</p> <p>Adobe Flash Player の脆弱性 (APSB15-18) に関する注意喚起</p>

	<p>2015年7月 Microsoft セキュリティ情報（緊急 4件含）に関する注意喚起</p> <p>マイクロソフト セキュリティ情報（MS15-078）に関する注意喚起</p> <p>ISC BIND 9 サービス運用妨害の脆弱性（CVE-2015-5477）に関する注意喚起</p>
2015年8月	<p>2015年8月 Microsoft セキュリティ情報（緊急 4件含）に関する注意喚起</p> <p>Adobe Flash Player の脆弱性（APSB15-19）に関する注意喚起</p> <p>マイクロソフト セキュリティ情報（MS15-093）に関する注意喚起</p>
2015年9月	<p>ISC BIND 9 サービス運用妨害の脆弱性（CVE-2015-5986）に関する注意喚起</p> <p>2015年9月 Microsoft セキュリティ情報（緊急 5件含）に関する注意喚起</p> <p>Adobe Flash Player の脆弱性（APSB15-23）に関する注意喚起</p>
2015年10月	<p>2015年10月 Microsoft セキュリティ情報（緊急 3件含）に関する注意喚起</p> <p>Adobe Reader および Acrobat の脆弱性（APSB15-24）に関する注意喚起</p> <p>Adobe Flash Player の脆弱性（APSB15-25）に関する注意喚起</p> <p>Adobe Flash Player の脆弱性（APSB15-27）に関する注意喚起</p> <p>2015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</p>
2015年11月	<p>2015年11月 Microsoft セキュリティ情報（緊急 4件含）に関する注意喚起</p> <p>Adobe Flash Player の脆弱性（APSB15-28）に関する注意喚起</p>
2015年12月	<p>2015年12月 Microsoft セキュリティ情報（緊急 8件含）に関する注意喚起</p> <p>Adobe Flash Player の脆弱性（APSB15-32）に関する注意喚起</p> <p>ISC BIND 9 サービス運用妨害の脆弱性（CVE-2015-8000）に関する注意喚起</p>

（2） 活動概要（報告状況等の公表）

発行日：2016-01-14 [2015年10月1日～2015年12月31日]

発行日：2015-10-08 [2015年7月1日～2015年9月30日]

発行日：2015-07-14 [2015年4月1日～2015年6月30日]

発行日：2015-04-16 [2015年1月1日～2015年3月31日]

(3) JPCERT/CC レポート

[発行件数] 49 件

[取り扱ったセキュリティ関連情報数] 284 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。