平成３０年３月●日
国家公安委員会
総務大臣
経済産業大臣

不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況

１　趣旨

不正アクセス行為の禁止等に関する法律（平成11年法律第128号。以下「不正アクセス禁止法」という。）第10条第１項の規定に基づき、国家公安委員会、総務大臣及び経済産業大臣は、不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況を公表する。

参考：不正アクセス禁止法（抜粋） 第10条　国家公安委員会、総務大臣及び経済産業大臣は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に資するため、毎年少なくとも一回、不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況を公表するものとする。 ２・３（略）

２　公表内容

○　不正アクセス行為の発生状況

平成29年１月１日から同年12月31日までの不正アクセス行為の発生状況を公表する。

○　アクセス制御機能に関する技術の研究開発の状況

国家公安委員会、総務省又は経済産業省のいずれかに係るアクセス制御機能の研究開発の状況、募集・調査した民間企業等におけるアクセス制御機能の研究開発の状況をそれぞれ公表する。

３　掲載先（ウェブサイト）

○　国家公安委員会　http://www.npsc.go.jp/

○　総　務　省　http://www.soumu.go.jp/

○　経済産業省　http://www.meti.go.jp/netsecurity/

不正アクセス行為の発生状況

第１　平成29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

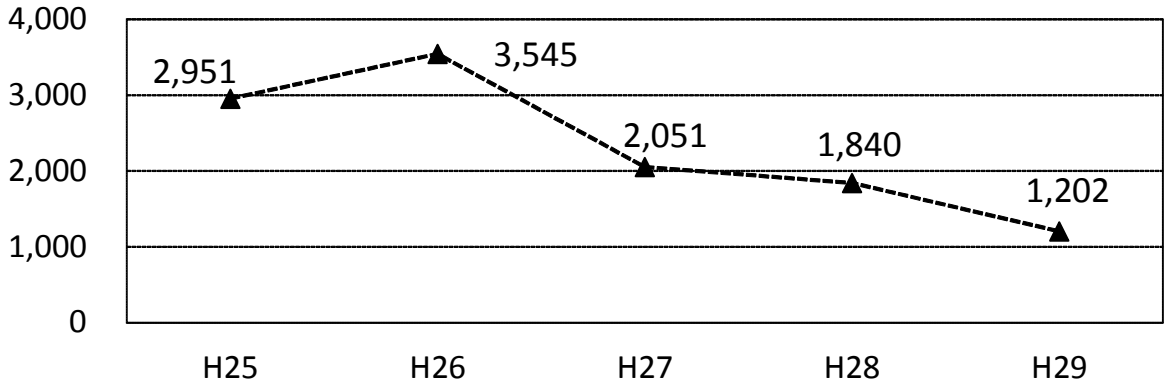
平成29年に都道府県警察から警察庁に報告のあった不正アクセス行為を対象とした。

１　不正アクセス行為の認知状況

(1)　認知件数

平成29年における不正アクセス行為の認知件数[注1]は1,202件であり、前年と比べ、638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1,177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25年	平成26年	平成27年	平成28年	平成29年
一般企業	2,893	3,468	1,998	1,823	1,177
行政機関等	24	3	14	5	9
プロバイダ	9	16	11	6	6
大学、研究機関等	9	56	11	2	5
その他	16	2	17	4	5
計(件)	2,951	3,545	2,051	1,840	1,202

※「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、「利用権者[注3]からの届出によるもの」が最も多く（655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」（283件）、「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」（255件）の順となっている。

図１－２　平成29年における認知の端緒別認知件数

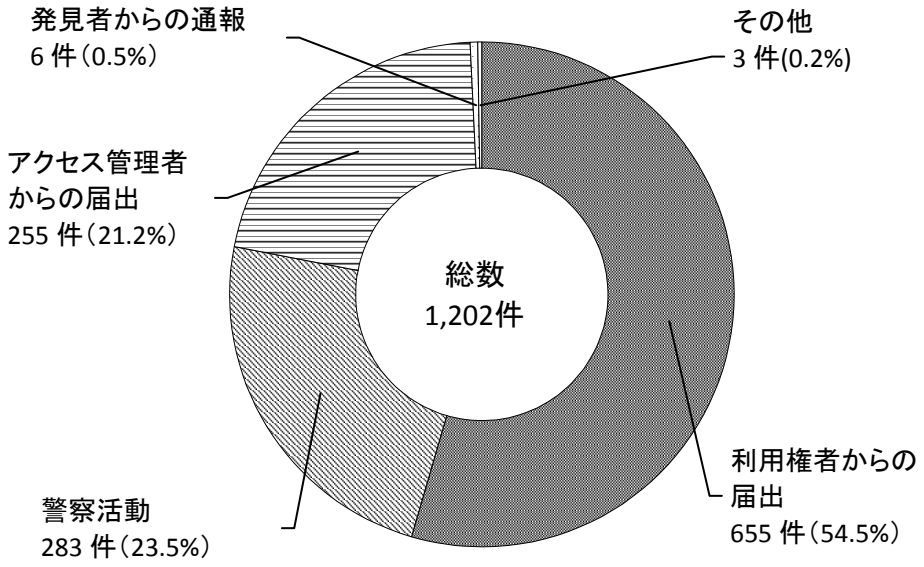


表１－２　過去５年の認知の端緒別認知件数

区分＼年次	平成25年	平成26年	平成27年	平成28年	平成29年
利用権者からの届出	929	1,337	614	495	655
警察活動	781	119	516	511	283
アクセス管理者からの届出	1,208	1,848	910	828	255
発見者からの通報	20	238	11	5	6
その他	13	3	0	1	3
計（件）	2,951	3,545	2,051	1,840	1,202

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等」が最も多く（442件）、次いで「仮想通貨交換業者等での不正送信」（149件）、「メールの盗み見等の情報の不正入手」（146件）の順となっている。

図１－３　平成29年における不正アクセス後の行為別認知件数

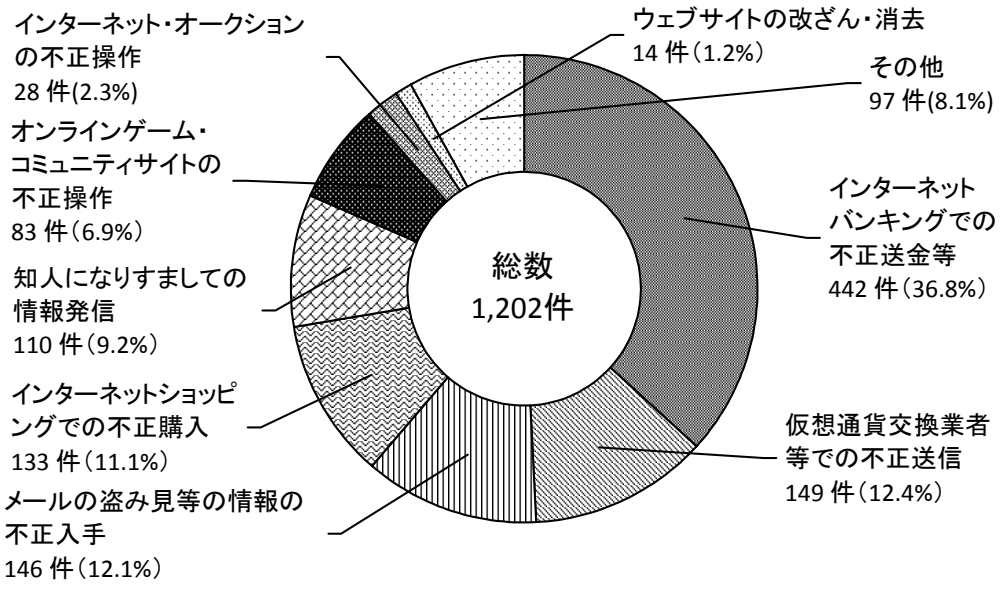


表１－３　過去５年の不正アクセス後の行為別認知件数

区分＼年次	平成25年	平成26年	平成27年	平成28年	平成29年
インターネットバンキングでの不正送金等	1,325	1,944	1,531	1,305	442
仮想通貨交換業者等での不正送信					149
メールの盗み見等の情報の不正入手	92	177	92	91	146
インターネットショッピングでの不正購入	911	209	167	172	133
知人になりすましての情報発信	26	1,009	83	25	110
オンラインゲーム・コミュニティサイトの不正操作	379	130	96	124	83
インターネット・オークションの不正操作	36	13	20	34	28
ウェブサイトの改ざん・消去	107	40	34	6	14
その他	75	23	28	83	97
計（件）	2,951	3,545	2,051	1,840	1,202

※　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29年における不正アクセス禁止法違反の検挙件数は648件、検挙人員は255人であり、前年と比べ、検挙件数は146件増加し、検挙人員は55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599件、242人、「識別符号の提供（助長）行為[注4]」が９件、12人、「識別符号の取得行為[注5]」が５件、５人、「識別符号の保管行為[注6]」が31件、６人、「フィッシング行為[注7]」が４件、４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25年	平成26年	平成27年	平成28年	平成29年
不正アクセス行為	検挙件数	968	338	332	462	599
	検挙事件数[注8]	142	141	154	175	216
	検挙人員	144	150	154	192	242
識別符号提供（助長）行為	検挙件数	7	0	5	5	9
	検挙事件数	7	0	5	2	6
	検挙人員	7	0	5	3	12
識別符号取得行為	検挙件数	2	16	10	6	5
	検挙事件数	1	5	1	3	3
	検挙人員	1	15	1	3	5
識別符号保管行為	検挙件数	2	2	12	28	31
	検挙事件数	2	2	2	6	2
	検挙人員	2	2	2	6	6
フィッシング行為	検挙件数	1	8	14	1	4
	検挙事件数	1	6	14	1	3
	検挙人員	1	6	14	1	4
計	検挙件数（件）	980	364	373	502	648
	検挙事件数（事件）	145（重複8）	150（重複4）	173（重複3）	182（重複5）	227（重複3）
	検挙人員（人）	147（重複8）	170（重複3）	173（重複3）	200（重複5）	255（重複14）

※　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　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545件、「セキュリティ・ホール攻撃型[注10]」が54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25年	平成26年	平成27年	平成28年	平成29年
識別符号窃用型	検挙件数	965	336	331	457	545
	検挙事件数	139	140	153	174	213
セキュリティ・ホール攻撃型	検挙件数	3	2	1	5	54
	検挙事件数	3	2	1	3	5
計	検挙件数（件）	968	338	332	462	599
	検挙事件数（事件）	142	141（重複1）	154	175（重複2）	216（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つ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」（92人）が最も多く、次いで「20～29歳」（87人）、「30～39歳」（36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13歳[注12]、最年長の者は60歳であった。

図３－１　平成29年における年代別被疑者数

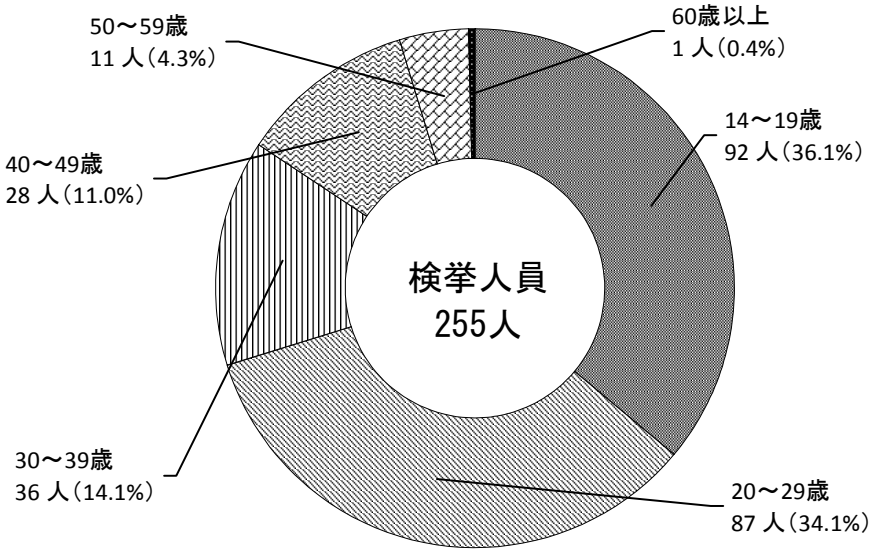


表３－１　過去５年の年代別被疑者数の推移

区分＼年次	平成25年	平成26年	平成27年	平成28年	平成29年
14～19歳	44	49	53	62	92
20～29歳	30	43	43	56	87
30～39歳	37	45	41	48	36
40～49歳	27	25	29	29	28
50～59歳	8	5	5	3	11
60歳以上	1	3	2	2	1
計（人）	147	170	173	200	255

(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（142人）、次いで「交友関係のない他人によるもの」（81人）、「ネットワーク上の知り合いによるもの」（32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（230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」（113件）、「他人から入手したもの」（74件）の順となっている。

図３－２　平成29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

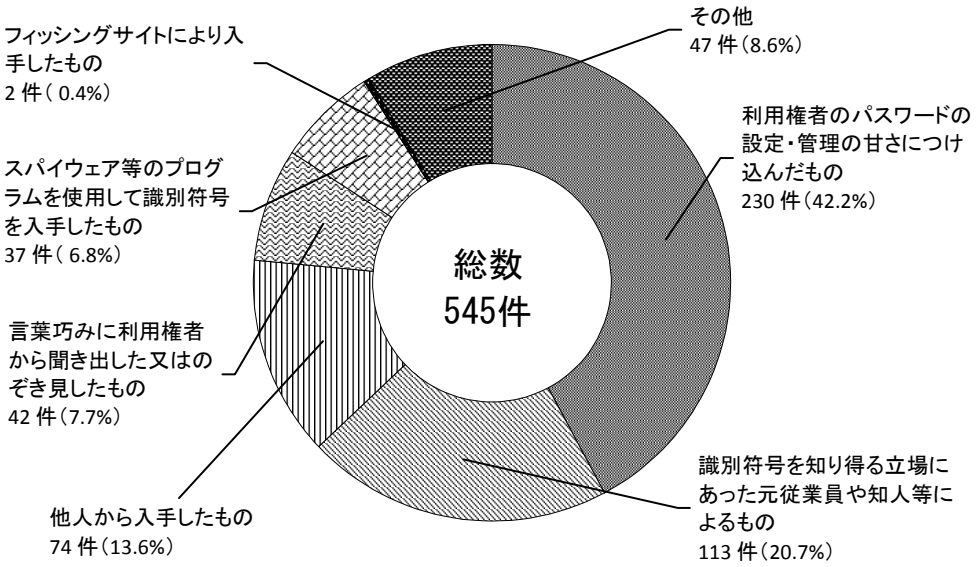


表３－２　過去５年の不正アクセス行為に係る手口別検挙件数

区分＼年次	平成25年	平成26年	平成27年	平成28年	平成29年
識別符号窃用型（件）	965	336	331	457	545
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	767	84	117	244	230
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	56	47	51	61	113
他人から入手したもの	33	25	13	20	74
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	64	53	46	49	42
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	25	6	15	34	37
フィッシングサイトにより入手したもの	9	71	24	3	2
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	9	34	57	4	0
その他	2	16	8	42	47
セキュリティ・ホール攻撃型（件）	3	2	1	5	54

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みると、「好奇心を満たすため」が最も多く（193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」（103件）、「不正に経済的利益を得るため」（93件）の順となっている。

図３－３　平成29年における不正アクセス行為に係る動機別検挙件数

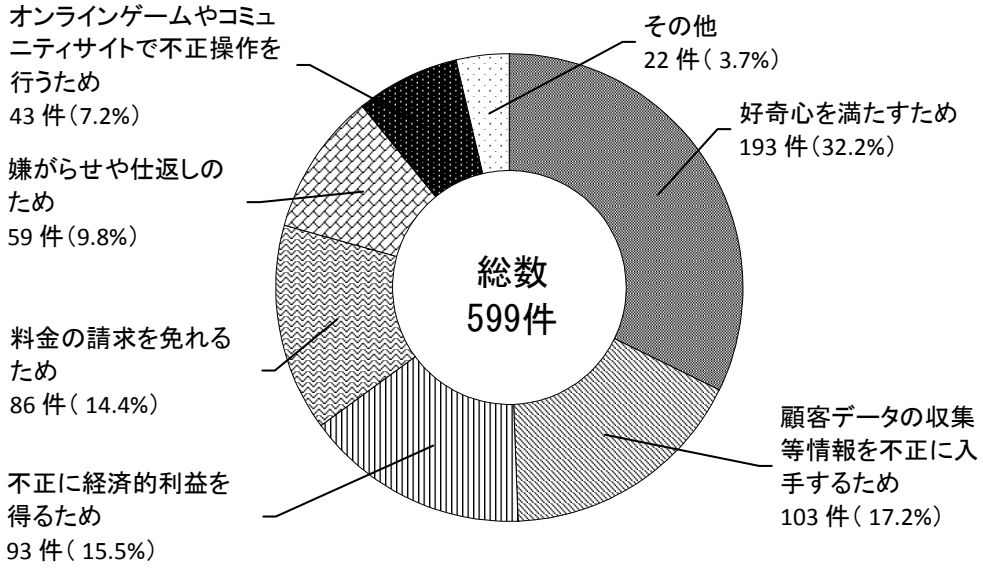


表３－３　過去５年の不正アクセス行為に係る動機別検挙件数

区分＼年次	平成25年	平成26年	平成27年	平成28年	平成29年
好奇心を満たすため	46	15	76	208	193
顧客データの収集等情報を不正に入手するため	53	139	72	70	103
不正に経済的利益を得るため	706	86	52	41	93
料金の請求を免れるため	25	2	58	25	86
嫌がらせや仕返しのため	56	54	44	44	59
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	77	41	28	43	43
その他	5	1	2	31	22
計（件）	968	338	332	462	599

(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（545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（210件）、次いで「社員・会員用等の専用サイト」（116件）、「電子メール」（92件）の順となっている。

図３－４　平成29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

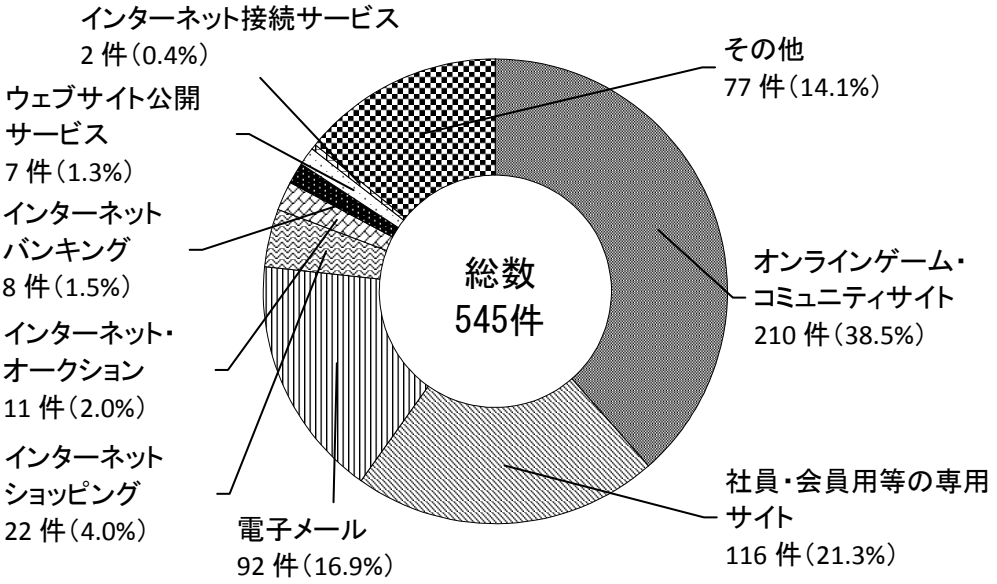


表３－４　過去５年の不正に利用されたサービス別検挙件数

区分＼年次	平成25年	平成26年	平成26年	平成28年	平成29年
識別符号窃用型　（件）	965	336	331	457	545
オンラインゲーム・コミュニティサイト	138	69	116	185	210
社員・会員用等の専用サイト	15	65	20	40	116
電子メール	48	30	64	136	92
インターネットショッピング	728	44	54	18	22
インターネット・オークション	5	15	20	9	11
インターネットバンキング	7	20	30	13	8
ウェブサイト公開サービス	6	7	9	2	7
インターネット接続サービス	0	11	11	5	2
その他	18	75	7	49	77

４　検挙事例

(1)　中国人の男（26）らは、平成28年10月から同年11月までの間、大手ポイントサイト及び家電量販店サイトに対し、不正に取得した各サイト利用者のＩＤ・パスワードを使用して不正アクセスし、不正に入手したポイントを利用してドラッグストア及び家電量販店において商品をだまし取った。平成29年５月から同年９月までに、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）。

(2)　高校生の少年（16）は、平成28年７月から同年10月までの間、 他人のＩＤ・パスワードをだまし取るため、ＳＮＳサイト等を模したフィッシングサイトをインターネット上に公開し、同サイトを閲覧した者にＩＤ・パスワードを入力させてこれらを詐取した。平成29年６月、不正アクセス禁止法違反（他人の識別符号を不正に取得する行為）で逮捕した（宮城・福井）。

(3)　地方公務員の男（39）は、平成27年５月から平成28年３月までの間、不正に入手した同僚職員のＩＤ・パスワードを使用して、自己の欲求を満たすため、職場の業務ネットワークシステムに不正アクセスし、同僚職員のメールを盗み見た。平成29年６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（新潟）。

(4)　美容師の男（32）は、平成29年１月、自ら新規開店した美容室の集客のため、以前勤務していた美容室が利用している顧客等管理システムに不正アクセスし、顧客情報を不正に取得するとともに、顧客の予約時には自らのメールアドレスに情報が送信されるよう設定した。同年８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（千葉）。

(5)　自営業の男（39）らは、平成29年１月、個人間の融資を仲介しているインターネット掲示板に、融資希望者に対して融資をする旨の虚偽の情報を書き込み、応募者に本人確認審査と称して、携帯電話のキャリア決済に必要なＩＤ・パスワードを送信させた上、これを使用して携帯電話会社決済用サーバに不正アクセスし、電子マネーをだまし取った。同年10月、不正アクセス禁止法違反（不正アクセス行為）で逮捕した（北海道）。

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29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約４割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及び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]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、仮想通貨交換業者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又は二経路認証・二要素認証の導入等に

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。

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。

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[注17]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。

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29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79件（平成28年：83件）であった。（注２）

平成29年は同28年と比べて、４件（約4.9%）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28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55件（平成28年：40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。

11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。

20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：16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24件の届出があった。

【主な内容】

ファイル等の改ざん、破壊等：18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、12件（平成28年：７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、20件（平成28年：40件）の届出があった。

【主な内容】

正規ユーザへのなりすまし：10件

メール不正中継：3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。

79件の届出中、実際に被害に遭った計54件（平成28年：61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：20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：５件

原因不明：11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：15 件
ファイアウォール：２件
不明：17 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

79 件の届出を被害内容で分類した 87 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 52 件（平成 28 年： 54 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】

ホームページ改ざん：12 件
データの窃取や盗み見：11 件
サービス低下：９件
踏み台として悪用：７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 29 年でも、依然として不正ログイン被害が多いことが見受けられる。不正アクセス届出において、被害に遭った 54 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 20 件（約 37.0%）と、大きな割合を占めている。また、被害に遭った 54 件のうち「メールサーバ」が被害に遭った届出は 12 件（約 22.2%）とあり、メールのアカウントを狙った攻撃が多かったことがわかる。スパムメールやばらまき型メールの踏み台ということだけでなく、BEC（ビジネスメール詐欺）の被害が確認されたところから、メールあるいは取引内容の窃取を目的としていることも推測される。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）
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 29 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 18,450 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 19,767 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 10,371 件の報告があった。
[1/1-3/31:2,391 件、4/1-6/30:3,447 件、7/1-9/30:2,554 件、10/1-12/31: 1,979 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 1,958 件の報告があった。
[1/1-3/31: 967 件、4/1-6/30: 461 件、7/1-9/30: 254 件、10/1-12/31: 276 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 336 件の報告があった。
[1/1-3/31: 91 件、4/1-6/30: 59 件、7/1-9/30: 98 件、10/1-12/31: 88 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 93 件の報告があった。

[1/1-3/31: 75 件、4/1-6/30: 3 件、7/1-9/30: 7 件、10/1-12/31: 8 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 3,306 件の報告があった。

[1/1-3/31: 707 件、4/1-6/30: 736 件、7/1-9/30: 1011 件、10/1-12/31: 852 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 77 件の報告があった。

[1/1-3/31: 4 件、4/1-6/30: 27 件、7/1-9/30: 13 件、10/1-12/31: 33 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 36 件の報告があった。

[1/1-3/31: 11 件、4/1-6/30: 9 件、7/1-9/30: 7 件、10/1-12/31: 9 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 3,590 件の報告があった。

[1/1-3/31: 610 件、4/1-6/30: 623 件、7/1-9/30: 867 件、10/1-12/31: 1490 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]

2017 年 1 月	2017 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 に対する複数の脆弱性に関する注意喚起 2017 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 (APSB17-02) に関する注意喚起 Adobe Reader および Acrobat の脆弱性 (APSB17-01) に関する注意喚起
2017 年 2 月	Adobe Flash Player の脆弱性 (APSB17-04) に関する注意喚起 ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2017-3135) に関する注意喚起 WordPress の脆弱性に関する注意喚起
2017 年 3 月	USB ストレージに保存されたデータを窃取するサイバー攻撃に関する注意喚起 (公開) 2017 年 3 月 Microsoft セキュリティ情報 (緊急 9 件含) に関する注意喚起 Adobe Flash Player の脆弱性 (APSB17-07) に関する注意喚起 Apache Struts 2 の脆弱性 (S2-045) 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
2017 年 4 月	2017 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 ISC BIND 9 に対する複数の脆弱性に関する注意喚起 2017 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 Reader および Acrobat の脆弱性 (APSB17-11) に関する注意喚起 Adobe Flash Player の脆弱性 (APSB17-10) に関する注意喚起
2017 年 5 月	ランサムウエア "WannaCrypt" に関する注意喚起 2017 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 Flash Player の脆弱性 (APSB17-15) に関する注意喚起
2017 年 6 月	ISC BIND 9 の脆弱性に関する注意喚起 インターネット経由の攻撃を受ける可能性のある PC やサーバに関する注意喚起 2017 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 (APSB17-17) に関する注意喚起

2017年7月	2017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 Cisco WebEx Browser Extension の脆弱性（CVE-2017-6753）に関する注意喚起 ISC BIND 9 の脆弱性に関する注意喚起 2017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 Adobe Flash Player の脆弱性（APSB17-21）に関する注意喚起 Apache Struts 2 の脆弱性（S2-048）に関する注意喚起
2017年8月	2017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
2017年9月	Apache Tomcat における脆弱性に関する注意喚起 Bluetooth の実装における脆弱性 "BlueBorne" に関する注意喚起 2017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（APSB17-28）に関する注意喚起 NTT ドコモ Wi-Fi STATION L-02F の脆弱性に関する注意喚起 Apache Struts 2 の脆弱性（S2-052）に関する注意喚起
2017年10月	2017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（APSB17-32）に関する注意喚起 2017 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
2016年11月	2017 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 macOS High Sierra の設定に関する注意喚起 2017 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 Reader および Acrobat の脆弱性（APSB17-36）に関する注意喚起 Adobe Flash Player の脆弱性（APSB17-33）に関する注意喚起
2017年12月	Mirai 亜種の感染活動に関する注意喚起 2017 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 Flash Player の脆弱性（APSB17-42）に関する注意喚起 Microsoft Malware Protection Engine のリモートでコードが実行

	される脆弱性（CVE-2017-11937）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] 52 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。

アクセス制御機能に関する技術の研究開発の状況

１　国で実施しているもの

総務省又は経済産業省が取り組むアクセス制御機能の研究開発に関してとりまとめたものであり、具体的には、独立行政法人自ら又は委託による研究、国からの委託又は補助による研究である。

実施テーマは以下の２件であり、その研究開発の概要は、別添１のとおりである。

Ｗｅｂ媒介型攻撃対策技術の実用化に向けた研究開発
HTTP相互認証プロトコル

２　民間企業等で研究を実施したもの

(1)　公募

警察庁、総務省及び経済産業省が平成29年12月８日から平成30年１月26日までの間にアクセス制御機能に関する技術の研究開発状況の募集を行ったところ、次のとおり１者から計１件の提案があった。それぞれの研究開発の概要は、別添２のとおりである。

なお、別添２の内容は当該企業から応募のあった内容を原則としてそのまま掲載している。

甲賀電子株式会社

(2)　調査

警察庁が平成29年10月から11月にかけて実施したアンケート調査に対し、アクセス制御技術に関する研究開発を実施しているとして回答のあった大学及び企業は次のとおりである。

ア　大学（６大学）

国士舘大学
関西大学
佐賀大学（３件）
日本大学
長崎大学（３件）
名古屋大学

イ　企業（２社）

株式会社ラック
ジャパンシステム株式会社

また、それぞれの研究開発の概要は別添３のとおりである。

なお、別添３の内容は、アンケート調査の回答内容を原則としてそのまま掲載している。

アンケート調査は、以下の条件に該当する大学及び企業の中から、調査対象として無作

為抽出した大学330校、企業1,270社の計1,600団体を対象に実施した。

・大学

国公立・私立大学のうち、理工系学部又はこれに準ずるものを設置するもの

・企業

市販のデータベース（四季報）に掲載された企業であって、業種分類が「情報・通信」「サービス」「電気機器」「金融」であるもの

（別添１）

対象技術　インシデント分析技術

テーマ名　Ｗｅｂ媒介型攻撃対策技術の実用化に向けた研究開発

開発年度　平成28年度～平成32年度

実施主体　株式会社KDDI総合研究所、国立大学法人横浜国立大学、他
（国立研究開発法人情報通信研究機構が実施する委託研究の委託先）

法人番号　5030001055903（KDDI総合研究所）、6020005004971（横浜国立大学）

背景、目的

Ｗｅｂを媒体としたサイバー攻撃は拡大の一途を辿っており、情報処理推進機構（ＩＰＡ）が公表している「情報セキュリティ　１０大脅威　２０１５」においても、Ｗｅｂ系の脅威が約半数を占め、国民の関心は高い。平成２７年６月に公表された日本年金機構からの年金情報流出においては、不正なＷｅｂサイトへの誘導も行われたと報道されており、Ｗｅｂ系の脅威とその対策は依然、重要課題である。

また、従来からあるＷｅｂの改ざんや「ドライブ・バイ・ダウンロード攻撃」に加え、標的型攻撃にＷｅｂサーバを利用する「水飲み場攻撃（watering hole attack）」や、オンラインバンキングユーザを狙ってＷｅｂブラウザ経由で情報を窃取する「バンキングマルウェア」、検索エンジン経由で不正なＷｅｂサイトに誘導する「ＳＥＯ（Search Engine Optimization）ポイゾニング」など、攻撃手法が多様化・複雑化してきている。さらに、攻撃対象がＷｉｎｄｏｗｓ　ＯＳのみならず、Ｍａｃ　ＯＳやＡｎｄｒｏｉｄ等のモバイル端末、ＩｏＴ機器（Ｌｉｎｕｘ組込み系機器）にまで広がってきており、重大な社会問題となっている。

そこで、これまで機構が委託研究として取り組んできた「ドライブ・バイ・ダウンロード攻撃対策フレームワークの研究開発」（平成24年度～平成27年度）を実用化に向けてさらに発展させ、観測対象をＷｉｎｄｏｗｓ　ＯＳのみならず、Ｍａｃ　ＯＳやモバイル端末、ＩｏＴ機器等に拡大するとともに、Ｗｅｂを媒体とした新たなサイバー攻撃への抜本的な対策に資する観測・分析・対策技術を確立する。

研究開発状況（概要）

平成28年度より以下の研究開発を開始、平成30年度に実施予定の実証実験に向けて研究開発は予定通り進捗中。平成32年度に終了予定だが、平成30年度に中間評価を行い、平成31年度以降の契約延長の可否を判定する。

（１）新型ブラウザセンサの研究開発
（２）新型観測機構の研究開発
（３）新型攻撃情報分析基盤の研究開発
（４）Ｗｅｂ媒介型攻撃対策技術の実証実験

詳細の入手方法（関連部署名及びその連絡先）

国立研究開発法人情報通信研究機構 イノベーション推進部門 委託研究推進室
（http://www.nict.go.jp/collabo/commission/itaku_kadai_h28.html）
電話 042－327－6011

将来の方向性

上記セキュリティ対策技術を確立し、高度情報通信ネットワーク社会の安全性・信頼性の確保に資する。

対象技術　高度認証技術

テーマ名　HTTP相互認証プロトコル

開発年度　平成17年度～

実施主体　国立研究開発法人　産業技術総合研究所
法人番号　7010005005425

背景、目的

HTTP相互認証プロトコルは､Webシステムでのフィッシング攻撃を防止するための新しい認証プロトコルです。

この認証プロトコルはPAKEと呼ばれる暗号･認証技術に新たな手法で改良を加え、Webの標準プロトコルであるHTTP及びHTTPSに適用したもので､ユーザがパスワードでサイトの真偽性を確認できる仕組みを提供することによって、フィッシングの防止を実現します。

研究開発状況（概要）

HTTP および HTTPS 上でのこれまでの標準認証技術である BASIC､DIGEST 認証法のフレームワークを拡張した形で、サーバがユーザを認証し、ユーザ側ではブラウザがサーバを自動的に認証するという､相互認証プロトコルを開発しました｡これら認証は､ユーザのパスワードに関する情報が正しいサーバには登録されていて、偽サーバには無いことを利用して行われています。

開発したプロトコルの仕様が､インターネット技術の標準化を行っている IETF から3つの標準文書として発行されました(RFC 8053: HTTP Authentication Extensions for Interactive Clients, RFC 8120: Mutual Authentication Protocol for HTTP, RFC 8121: Mutual Authentication Protocol for HTTP: Cryptographic Algorithms Based on the Key Agreement Mechanism 3 (KAM3))｡また技術を体験してもらうためのサーバ実装､Firefox､Chromium ベースのブラウザ（クライアント）の試験実装を公開しています。

詳細の入手方法（関連部署名及びその連絡先）

独立行政法人産業技術総合研究所　情報技術研究部門
TEL: 029-862-6600
URL:https://www.itri.aist.go.jp/

将来の方向性

IETFで標準化されたHTTP相互認証プロトコルの仕様の普及を図り、開発技術がブラウザの標準機能として搭載されることを目指します。これにより､認証機能を個々のWebアプリケーションで作りこまなくても安全に実現することが可能になることから、偽サーバによる情報詐取被害の防止に貢献していきます。

（別添２）

企業名（及び略称）：甲賀電子株式会社 法人番号：9160001005362	
代表者氏名：代表取締役　中沼　忠司	
所在地（郵便番号及び住所）：〒520-3047　滋賀県栗東市手原5-8-10	
関連部署名及び電話番号：営業技術課　077-552-5123	
ＵＲＬ：http://www.koga.co.jp	
対象技術	技術開発状況
（注１） ・侵入検知・防衛技術 ・ぜい弱性対策技術 ・高度認証技術 開発年：2013年～2017年	【技術概要】 成り済ましによる侵入を防ぐ技術の提案です。 現状のインターネットの網機能（TCP/IP）は変更せず、ルーター・ホスト等の端末側のプロトコルを変更する軽微なソフト修正により実現します。 既存のIoTシステムには、通信回線と通信端末の間に本技術を実行するセキュリティ･ゲートウェイを設置することで､サイバー攻撃から保護します。 接続を許容するIPアドレスを予め登録しておき､正しい送信元の通信回線とは相互に回線認証して接続し､IPアドレスを偽証する発信者の通信回線とは１バイトのデータも授受せずに切断して侵入を防ぎ､不正アクセスを排除します。 【開発状況】 試作機を完成させ、本技術が有効に機能することを確認済み。 【工業所有権】 国際特許を出願済み、日本は特許査定。以後各国の特許を取得する予定。

（別添３）

ア　大学

企業・大学名	国士舘大学　理工学部
代表者名	理工学部長　二川　佳央
所在地	東京都世田谷区世田谷4-28-1
窓口部署名	
電話番号	03-5481-3251
関連部門名	国士舘大学　理工学部
ホームページのURL	
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： 特になし 研究開発国： 日本 研究開発時期： 平成28年4月1日～平成29年7月31日	学内の論文誌（紀要）にて発刊予定のレベル。

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	