平成29年３月23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28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/menu_news/s-news/01ryutsu03_02000119.html
○　経済産業省　http://www.meti.go.jp/policy/netsecurity/index.html

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

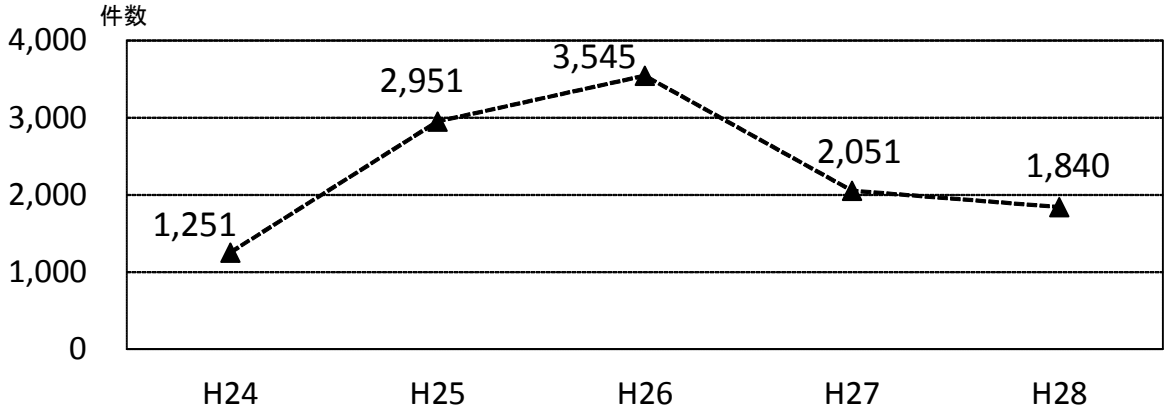
平成28年に都道府県警察から警察庁に報告のあった不正アクセス行為を対象とした。

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

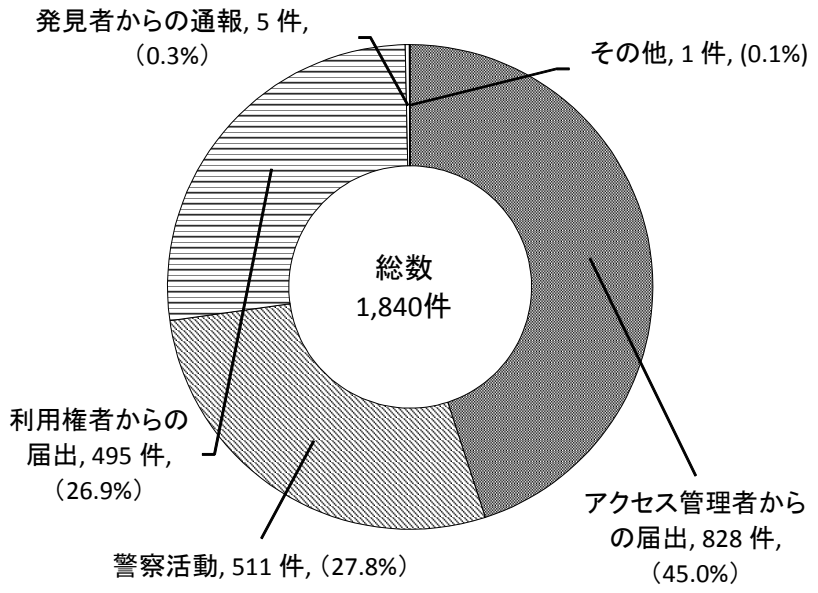


表１－２　過去５年の認知の端緒別認知件数

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

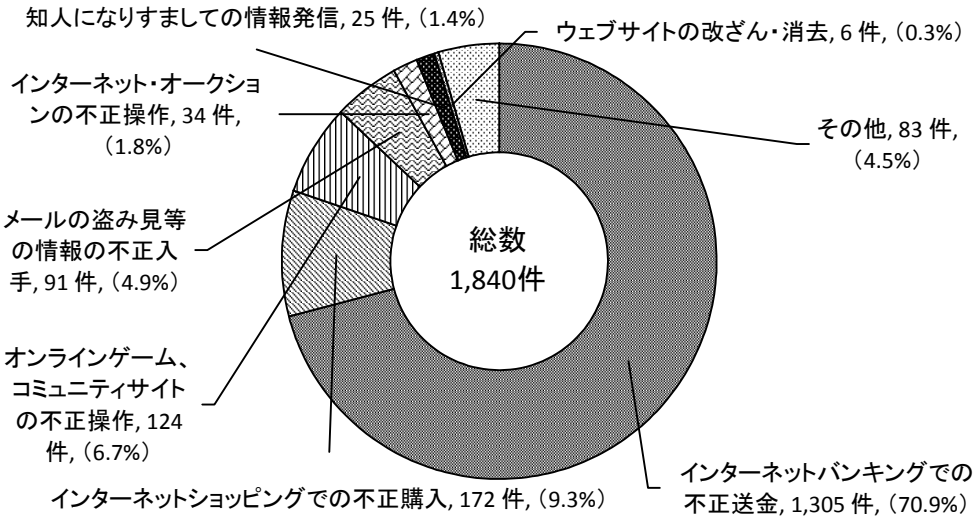


表１－３　過去５年の不正アクセス後の行為別認知件数

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

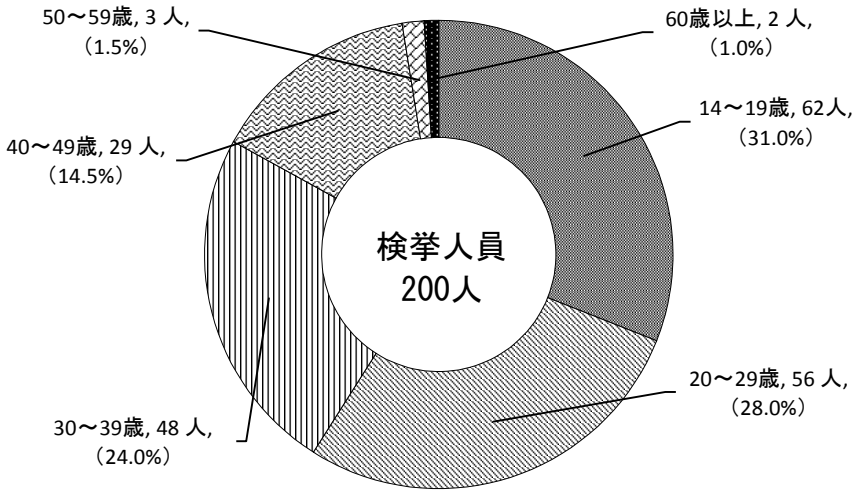


表３－１　過去５年の年代別被疑者数の推移

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

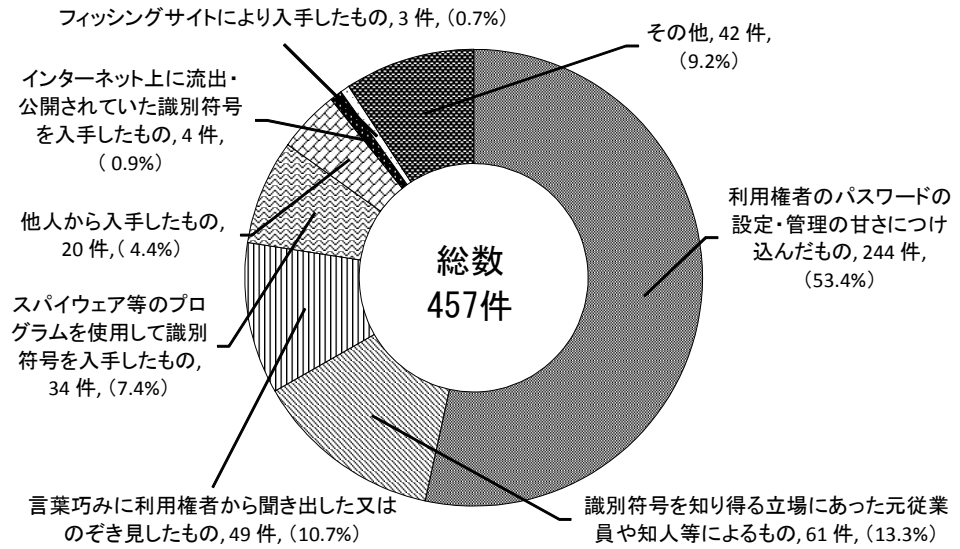


表３－２　過去５年の不正アクセス行為に係る手口別検挙件数

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

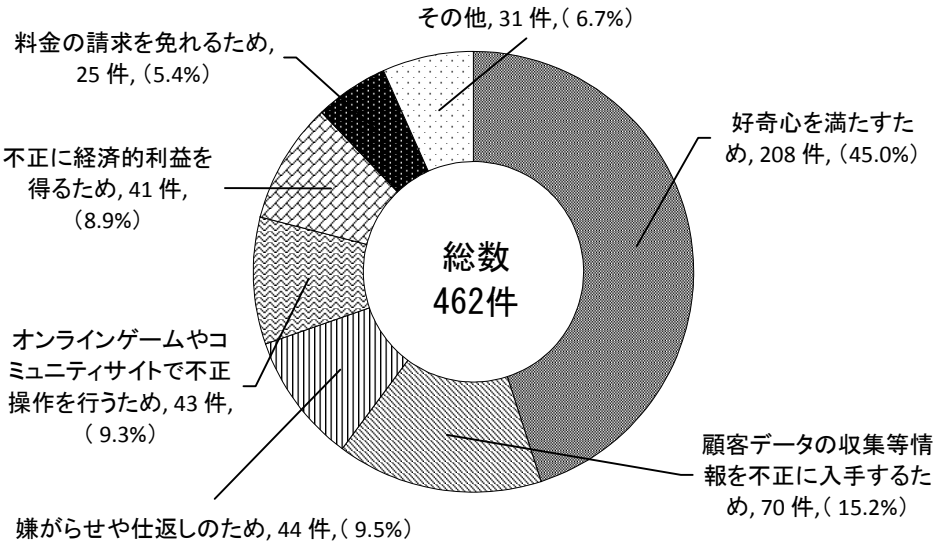


表３－３　過去５年の不正アクセス行為に係る動機別検挙件数

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

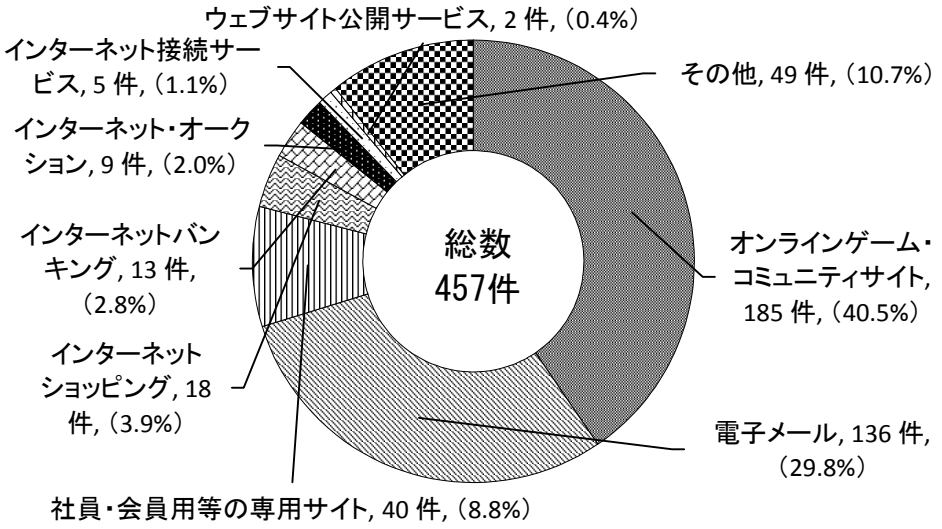


表３－４　過去５年の不正に利用されたサービス別検挙件数

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。

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４件であり、その研究開発の概要は、別添１のとおりである。

サイバーセキュリティ技術の研究開発
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
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28年12月９日から平成29年１月27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４者から計４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。

イーロックジャパン株式会社
株式会社ギデオン
サイエンスパーク株式会社
フューチャーアーキテクト株式会社

(2)　調査

警察庁が平成28年８月から９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）

秋田大学
大阪府立大学
佐賀大学
東京情報大学
徳島大学
名城大学

イ　企業（２社）

アラクサラネットワークス株式会社
株式会社東京商工リサーチ（３件）

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325校、企業1,286社の計1,611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、IT総覧等）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　サイバーセキュリティ技術の研究開発

開発年度　平成18年度～

実施主体　国立研究開発法人情報通信研究機構
法人番号　7012405000492

背景、目的

サイバー攻撃の急増と被害の深刻化によりサイバーセキュリティ技術の高度化が不可欠となっていることから、ネットワークを介したサイバー攻撃やマルウェア等の活動を大局的に把握・対応するための各種観測技術、分析技術、可視化等の研究開発を行う。

研究開発状況（概要）

これまでに研究開発・整備したサイバー攻撃観測機構や、マルウェアの収集・分析機構に関して、世界規模の観測網確立に向けた観測規模の更なる拡充、より高度な観測・分析機構の開発等を行った。観測・分析結果については、Webサイト等で広く公開するとともに、アラートシステム等の外部への技術移転を行った。また、地方自治体へのアラート提供を拡大する等、研究開発成果の社会展開を推進した。

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　サイバーセキュリティ研究所　サイバーセキュリティ研究室　042-327-6225

将来の方向性

上記の研究開発を通じて、将来のネットワーク自身及びネットワーク上を流通する情報の安全性・信頼性の確保と、利用者にとって安全・安心な情報通信基盤の実現を目指す。

対象技術　インシデント分析技術

テーマ名　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

開発年度　平成24年度～平成27年度

実施主体　株式会社KDDI研究所、株式会社セキュアブレイン
（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研究所）、3010001090029（セキュアブレイン）

背景、目的

近年、攻撃者の改竄によって多くのWeb サイトに悪性サイトへのリダイレクト命令を埋め込まれ、それらサイトにアクセスしたユーザが悪性サイトへ誘導されてマルウェアに感染するといった被害が拡大している。これは、ブラウザやプラグインの脆弱性を悪用し、強制的にマルウェアをダウンロード・実行させるドライブ・バイ・ダウンロード攻撃（Drive-by-Download attack：以下DBD 攻撃）が原因である。

このDBD 攻撃は従来のリモートエクスプロイト攻撃とは異なり、ユーザのWeb アクセスを攻撃の起点とするため、ダークネット観測のような従来の受動的な攻撃観測手法ではその脅威を捉えられない。一方、能動的にWeb サイトをクローリングし検査を行うクライアントハニーポットのようなシステムを用いて、検知した悪性サイトのURL をブラックリストとして提供することで攻撃を防止する対策手法も存在する。しかし膨大な数のWeb サイトが存在し、なおかつ悪性サイトはそのURL を短期間で遷移させているという状況において、効果的な対策とするためには、シード（クローリングの起点）をどこに設定するかという問題点と、如何に検査したURL の鮮度を保つか（再検査までの期間を短くするか）という問題点が存在するなど、セキュリティ分野で未だ決定打となる対策が打ち出せていない状況が続いている。

本研究開発では、機構が検討してきた基本アーキテクチャ及びプロトタイプを踏まえた上で、DBD 攻撃についてその脅威を解明し、安心・安全なネットワーク社会の実現に向け、DBD 攻撃対策フレームワークの確立に資することを目指す。

研究開発状況（概要）

平成24年度より以下の研究開発を開始し平成27年度に終了。

（１）DBD攻撃大規模観測網構築技術
（２）DBD攻撃分析・対策技術
（３）DBD攻撃対策フレームワーク実証実験

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_h27.html）
電話 042－327－6011

将来の方向性

上記セキュリティ技術を確立し、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　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し、平成32年度に終了予定。但し、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。

これまでプロトコルを3つの文書で記述し、インターネット技術の標準化を行っている IETF での標準化提案を行いました。現在 HTTPAUTH WG で標準化の議論が行われており、議論の結果に基づき、サーバ実装、Firefox、Chromium ベースのブラウザ（クライアント）実装を改良してきました。平成29年1月に、標準化案3つのうちの1つで、提案プロトコルで必要となるパラメータ等を規定する文書が、RFC 8053 HTTP Authentication Extensions for Interactive Clientsとして標準化されました。

詳細の入手方法（関連部署名及びその連絡先）

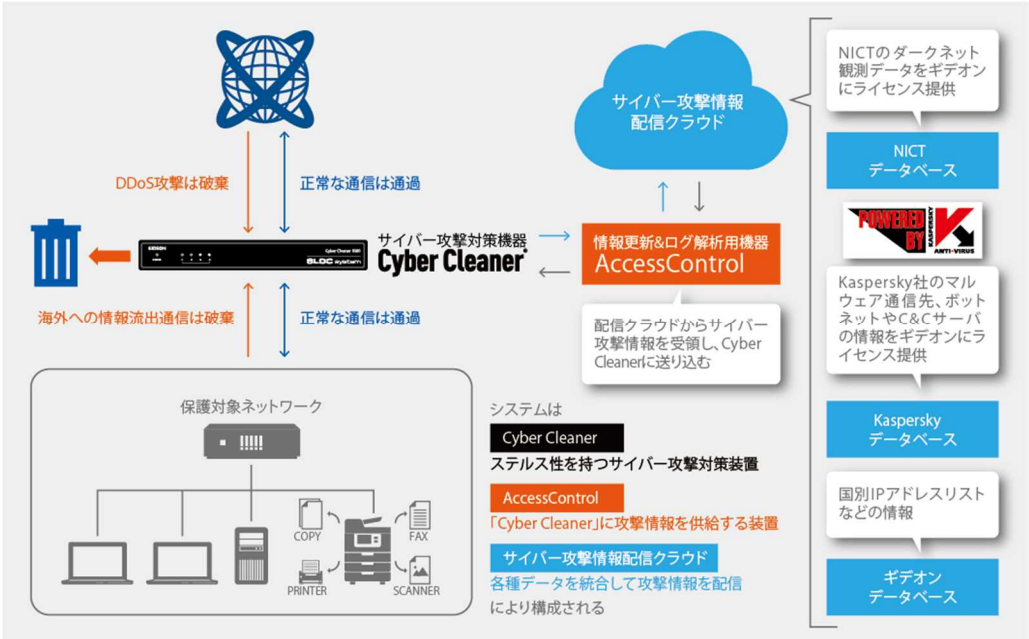
独立行政法人産業技術総合研究所　情報技術研究部門
TEL:029-861-5284
URL:http://www.itri.aist.go.jp/

将来の方向性

IETFで引き続き残りの2つの文書を標準化し、HTTP相互認証プロトコルが標準機能としてブラウザに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）：イーロックジャパン株式会社 法人番号：9010001131875	
代表者氏名：秦　基嘉	
所在地（郵便番号及び住所）：〒102-0083　東京都千代田区麹町3-12-7	
関連部署名及び電話番号：セキュリティコンサルタント事業部　03-3265-1169	
ＵＲＬ：http://www.elock.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 ・その他アクセス制御機能に関する技術 WebALARM:2000年、The GRID Beacon：2011年	（注２） ■WebALARM 不正侵入、改竄等防御対策として開発されたセキュリティ対策ソフトウェアです。Server上のあらゆる静的ファイルをリアルタイムに監視し、万一不正に改竄された場合でも検知後瞬時に自動復旧を行い、管理者への警告、証拠保全するリカバリーツールです。データアップデートに関しても監視を止めず自動更新可能です。また、PCIDSS要件10.5.5、11.5にも対応しております。 ■The GRID Beacon フィッシング手法、ＤＮＳ改竄による別サイトへの誘導やMITM、 MITB等あらゆる危険を完全に排除する2経路/2要素認証システムです。スマートフォンを強力なアウトオブバンド・マルチファクタ認証装置として利用することで、OTP専用機器やマトリクス表等といった複雑な認証要素は不要となり、低コストで老若男女を問わず利便性のよい強固なセキュリティを実現します。 また追加機能として、顔認証、声紋パターン認証等生体認証にも対応します。

企業名（及び略称）株式会社ギデオン 法人番号　2020001019903	
代表者氏名 代表取締役　西尾　高幸	
所在地（郵便番号及び住所）〒223-0056 神奈川県横浜市港北区新吉田町3448-4	
関連部署名及び電話番号 総務部 電話番号:045-590-1216	
ＵＲＬ http://www.gideon.co.jp/	
対象技術	技術開発状況
・侵入検知・防御技術 ・ぜい弱性対策技術 ・インシデント分析技術 ・その他アクセス制御機能に関する技術 開発年: 平成２６年度～ 平成２７年度	(1)Cyber Cleaner(製品名) はゲートウェイ（もしくはルータ）の上位に設置し通信(PPPoE通信上)を判定し、攻撃(有害)通信を遮断することで下位のネットワークを保護する。このことで外部からの攻撃(DDoS攻撃などによる)及び内部からの情報流出(マルウエア感染などによる)を防ぐ。 (2)サイバー攻撃情報(NICTからライセンスされた情報、Kaspersky社からライセンスされた情報、及びギデオン社から提供する国別、ISP別情報など)は、最新情報としてギデオン社から毎時配信され、Cyber Cleanerに反映され最新のサイバー攻撃に即応する。 (3)Cyber CleanerはIPアドレスをもたないため、機器自体が攻撃を受けることがなく、また攻撃により停止しない。 (4)PPPoE通信及びVPN通信の経路上に導入設置できる唯一のサイバー攻撃対策機器*。 (5)TCPヘッダ解析で判定するため、どのような通信環境にでも対応可能で、かつ処理が高速に行える。 ＊20170106現在  	

企業名（及び略称）サイエンスパーク株式会社
法人番号　8021001026306

代表者氏名　小路　幸市郎

所在地（郵便番号及び住所）神奈川県座間市入谷3-1649-2

関連部署名及び電話番号　開発部SDK開発課　046-255-2544

ＵＲＬ　http://www.sciencepark.co.jp/

対象技術	技術開発状況
・その他アクセス制御機能に関する技術 平成13年～	「Driverwareセキュリティ SDK」は、エンドポイント向けの情報セキュリティシステムを開発する際に利用できるソフトウェア開発キットである。情報セキュリティ製品に必要な機能をOSの処理に近いカーネル層にて実現することで、情報流出経路の変化に対応する。近年はPCから各種スマートフォンへのデータ持ち出しを禁止する機能や、無許可のWi-Fi通信を禁止する等、新しいデバイスへの対応を行った。現在、Bluetooth通信の制御を開発中であり、今後も新しい情報流出経路への対応に取り組んでいく。 主要な機能は以下の通り。

ネットワーク制御	IPアドレス、ポート単位でのTCP/UDP通信制御、ログ収集、Wi-Fi通信の制御
ファイル制御	ファイルの読み込みと書込みの許可・禁止を制御
ファイルログ収集	ファイルアクセスのログ収集
ファイルの持ち出し承認機能	第三者による許可、禁止指示による、ファイルの持ち出しフロー
ライティング制御	CD、DVD、Blu-rayへの書き込み許可・禁止を制御、ログ収集
印刷制御	印刷の許可・禁止を制御、ログ収集
外部デバイス制御	iPhone、Android端末など、USB接続による携帯端末へのファイル持ち出し制御
暗号化制御	ファイル単位でのリアルタイム暗号化・復号
通信制御	シリアルや赤外通信などCOMポートの通信を制御します。
その他	キーボード等のHID（Human Interface Device）の入出力制御

＜＜製品概要＞＞
http://www.sciencepark.co.jp/information_security/sdk/summary.html

企業名（及び略称）フューチャーアーキテクト株式会社 法人番号　2010701032272	
代表者氏名　東 裕二	
所在地（郵便番号及び住所）〒141-0032 東京都品川区大崎1-2-2 ｱｰﾄｳﾞｨﾚｯｼﾞ大崎ｾﾝﾄﾗﾙﾀﾜｰ	
関連部署名及び電話番号　Technology Innovation Group / 03-5740-5723	
ＵＲＬ　http://www.future.co.jp/	
対象技術	技術開発状況
ぜい弱性対策技術 開発年： 平成28年度-平成29年度	国内のサイバー攻撃（標的型攻撃）による被害件数は年々増加しており、ソフトウェアやウェブアプリケーションの脆弱性への対応の遅れや漏れによるリスクは急速に高まっています。一方で新着の脆弱性情報は届け出のあるものだけで年間に約6000件を超え、それらをシステム管理者が手動で管理する負荷は高く、数百から数千のシステムを管理する場合にはとくに困難でした。 この課題を解決するために、当社はシステムが抱える保安上の欠陥に関する情報の収集と検知を全自動化した脆弱性スキャンツール「Vuls（VULnerability Scanner）」を開発し、2016年4月1日にオープンソース（*1）として無償で「GitHub」（*2）に公開いたしました。 「Vuls」は、オンプレミス環境とクラウド環境のどちらにも対応し、広範なソフトウェアの脆弱性をスキャンして日々発見される脆弱性がどのサーバに該当するかまで特定します。これにより管理者は脆弱性をリアルタイムに検知できるようになり、サイバー攻撃によるリスクを低減できます。また、内容や深刻度をひと目で把握できる日本語のレポートが発行され、システム管理者の負荷を大きく低減させます。 尚、「Vuls」は公開直後から世界中で話題となり、2016/10/1にGitHubスター獲得ランキング全言語第1位に入りました。またSlack（*3）コミュニティへの参加者も300名を超え、日々増加しています。 今後は、より広範なセキュリティ脅威に対応できるよう機能のブラッシュアップと拡張を図り、脆弱性スキャンツールのデファクトスタンダードを目指すとともに、エンタープライズ用途にも対応するサービスメニューとしての展開を目指します。 ＊1　オープンソースとは、ソースコードを広く一般に公開し、誰にでも無償で自由に扱えるようにしたソフトウェアのことを指します。 ＊2　「GitHub」はソフトウェア世界中の開発者のためのソースコード管理・共有を目的としたWebサービスです。 ＊3　「Slack」はチーム内でのコミュニケーションをとるためのチャットサービスです。 ※　「Vuls™」は、当社の親会社であるフューチャー株式会社が商標登録出願中です。 ■Vuls公開リポジトリ：　https://github.com/future-architect/vuls

（別添３）

ア　大学

企業・大学名	秋田大学理工学部
代表者名	村岡　幹夫
所在地	〒010－8502　秋田県秋田市手形学園町１－１
窓口部署名	総務担当
電話番号	018-889-2305
関連部門名	秋田大学　理工学部　数理・電気電子情報学科　人間情報工学コース
ホームページのURL	http://www.riko.akita-u.ac.jp/
研究説明のURL	http:www.ie.akita-u.ac.jp/
対象技術	技術の概要・特徴など
研究開発名称： 口唇の動き特徴を用いた個人認証 研究開発国： 日本 研究開発時期： 平成22年4月1日～平成31年3月31日	口唇の動き特徴から研究室レベル（20人程度）の個人認証が可能である

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	

企業・大学名	大阪府立大学　大学院　工学研究科
代表者名	辰巳砂　昌弘
所在地	〒599－8531　大阪府堺市中区学園町１－１
窓口部署名	共同研究，受託研究等に関するお問い合わせ研究連携推進課
電話番号	072-254-9107
関連部門名	電子透かし
ホームページのURL	http://www.eng.osakafu-u.ac.jp
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： 電子透かしを用いた改ざん検出と復元 研究開発国： 日本 研究開発時期：	あらかじめ，電子透かし技術を利用して画像に透かしを埋め込み，透かし入り画像を作成しておく．透かし入り画像に改ざんが施されたとしても，埋め込まれている透かしがどのように破壊されているかを確認することによって，どの領域が改ざんされたかを検出できる．その上，改ざんされる前の状態を，低解像度ではあるものの，復元可能である．

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	

企業・大学名	国立大学法人 佐賀大学
代表者名	
所在地	〒840－8502
窓口部署名	
電話番号	
ホームページのURL	http://www.saga-u.ac.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： Opengate, OpengateM 開発元(メーカー名等)： 佐賀大学 開発国： 日本 価格： オープンソース 発売時期： 出荷数：	無線LANや情報コンセントを利用する際に利用者を認証するためのシステムであり、Webによる平易なインターフェイスを持ち、特別なソフトウェアを導入することなく、利用可能です。利用者の認証終了後、ネットワークを利用することができ、利用終了後は即座に閉鎖します。IPv4のみだけでなく、IPv6にも対応しています。様々な認証方式に対応し、Shibbolethによるシングルサインオンにも対応しているのが特長です。また、Webによる認証と連携して、利用者のデバイスをMACアドレスで認証することも可能です。このACアドレス認証のためのデバイスの登録管理機能も有しています。Opengate http://www.cc.saga-u.ac.jp/opengate/

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	○

企業・大学名	東京情報大学
代表者名	学長　鈴木 昌治
所在地	〒265－8501 千葉市若葉区御成台4-1
窓口部署名	総務課
電話番号	043-236-4603
関連部門名	ネットワーク・セキュリティコース
ホームページのURL	http://www.tuis.ac.jp
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： ネットワークセキュリティ、情報ネットワーク技術に関する研究 研究開発国： 日本 研究開発時期：	

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	

企業・大学名	徳島大学理工学部
代表者名	河村　保彦
所在地	〒770－8506 徳島県徳島市南常三島町２丁目１番地
窓口部署名	常三島事務部理工学部事務課総務係
電話番号	088-656-7304
関連部門名	知能情報系・ネットワークシステム制御研究室
ホームページのURL	http://www.tokushima-u.ac.jp/st/
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： M2M/IoTネットワークにおけるアクセス制御 研究開発国： 日本 研究開発時期： 平成28年4月1日～	構想段階

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	○

企業・大学名	名城大学理工学部情報工学科　鈴木秀和研究室
代表者名	鈴木　秀和
所在地	〒　468－8502　名古屋市天白区塩釜口一丁目501番地
窓口部署名	理工学部事務室
電話番号	052-832-1151
関連部門名	理工学部
ホームページのURL	http://www.meijo-u.ac.jp/
研究説明のURL	http://www.ucl.meijo-u.ac.jp, http://www.ntmobile.net/
対象技術	技術の概要・特徴など
研究開発名称： NTMobile（Network Traversal with Mobility） 研究開発国： 日本 研究開発時期： 平成22年6月～	NTMobileとは，IPv4/IPv6混在ネットワークにおいて通信開始時に端末（PC，サーバ，スマートフォンのモバイル端末など）間で暗号鍵の交換および暗号化通信路を動的かつできる限りエンドツーエンドで構築する技術である．これまでに暗号化通信機能，通信相手認証機能，暗号鍵管理機能などの技術仕様を決定し，一部の機能についてはLinux，Android，iOSアプリとして実装が完了している．現在は企業と共同研究開発を進めており，研究開発成果をライブラリやサービスとして構築し，アプリケーション開発者などへ提供することを検討している．

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	

イ　企業

企業・大学名	アラクサラネットワークス株式会社
代表者名	南川育穂
所在地	〒212－0058　川崎市幸区鹿島田１－１－２　新川崎三井ビル　西棟
窓口部署名	
電話番号	
ホームページのURL	http://www.alaxala.com/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： AXシリーズ（スイッチ、ルータ） 開発元(メーカー名等)： アラクサラネットワークス株式会社 開発国： 日本 価格： ¥81,000（AX620R-2105）～ 発売時期： 平成16年10月1日 出荷数： 累計　167,600台（2015年9月30日時点）	AXシリーズは、VLANによるネットワーク分離やACL(Access Control List)による通信制御といった基本的なセキュリティ機能に加え、アクセス制御に関わる以下の特徴的な機能で安心なネットワークを提供します。1. ホワイトリスト機能 ネットワーク上の通信を学習し、自動で許可リストを作成。運用中は、ネットワークに上の全ての通信を監視。許可リストにない不正な通信を全てシャットアウトすることで、様々な攻撃からネットワークを効果的に守る。 対象モデル： AX2500S、AX260A2. トリプル認証IEEE802.1X認証/Web認証/MAC認証） 様々な端末が混在した環境でも、端末に応じた認証を利用可能。また、複数端末を集線するハブ経由でも認証が可能なため、コストパフォーマンスの高いネットワークを構築可能。対象モデル：AX8600S、AX8300S、AX8600R、AX620Rを除く全モデル3. セキュア仮想ネットワーク単一の物理機器上でネットワークを仮想的に分離する。ネットワーク上のトラフィックを分けることが可能なため、物理構成に囚われないセキュリティの確保が可能。また、機器の集約が可能なため、コスト低減も可能。対象モデル：AX2500S、AX2200S、AX1200S、AX260A、AX620Rを除く全モデル

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	

企業・大学名	株式会社　東京商工リサーチ
代表者名	代表 取締役 取締役 社長 河原 光雄
所在地	〒 100-6810　東京都千代田区大手町 1-3-1 JA ビル
窓口部署名	システム 本部
電話番号	03-6910-3160
ホームページのURL	http://www.tsr-net.co.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： ウイルスバスター 開発元(メーカー名等)： トレンドマイクロ株式会社 開発国： 日本 価格： 発売時期： 出荷数：	

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	○

企業・大学名	株式会社　東京商工リサーチ
代表者名	代表 取締役 取締役 社長 河原 光雄
所在地	〒 100-6810　東京都千代田区大手町 1-3-1 JA ビル
窓口部署名	システム 本部
電話番号	03-6910-3160
ホームページのURL	http://www.tsr-net.co.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： IBM Aliss 開発元(メーカー名等)： 日本アイ・ビー・エム株式会社 開発国： 日本 価格： 発売時期： 出荷数： 	

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	○

企業・大学名	株式会社　東京商工リサーチ
代表者名	代表 取締役 取締役 社長 河原 光雄
所在地	〒 100-6810　東京都千代田区大手町 1-3-1 JA ビル
窓口部署名	システム 本部
電話番号	03-6910-3160
ホームページのURL	http://www.tsr-net.co.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： CISCO VPN-GW, Micorsoft Active Directory IIJ GIOリモートアクセス 開発元(メーカー名等)： シスコシステムズ合同会社, 日本マイクロソフト株式会社 株式会社インターネットイニシアチブ 開発国： 米国、米国、日本 価格： 発売時期： 出荷数：	

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	○