

令和2年3月5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31年1月1日から令和元年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/>

## 不正アクセス行為の発生状況

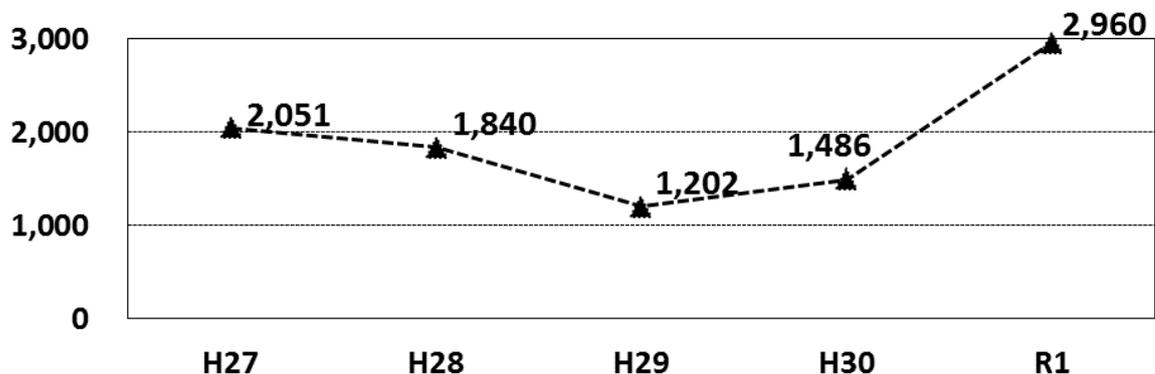
第1 令和元年における不正アクセス禁止法違反事件の認知・検挙状況等について  
令和元年<sup>注1</sup>に都道府県警察から警察庁に報告のあった不正アクセス行為を対象とした。

### 1 不正アクセス行為の認知状況

#### (1) 認知件数

令和元年における不正アクセス行為の認知件数<sup>注2</sup>は2,960件であり、前年と比較すると1,474件（約99.2%）増加した。

(件) 図1-1 過去5年の不正アクセス行為の認知件数の推移



#### (2) 不正アクセスを受けた特定電子計算機のアクセス管理者

不正アクセス行為の認知件数について、不正アクセスを受けた特定電子計算機のアクセス管理者<sup>注3</sup>別に内訳を見ると、「一般企業」が最も多く2,855件となっている。

表1-1 過去5年の不正アクセスを受けた特定電子計算機のアクセス管理者別認知件数

区分	年次	平成27年	平成28年	平成29年	平成30年	令和元年
一般企業		1,998	1,823	1,177	1,314	2,855
行政機関等		14	5	9	6	90
プロバイダ		11	6	6	4	6
大学、研究機関等		11	2	5	161	3
その他		17	4	5	1	6
計(件)		2,051	1,840	1,202	1,486	2,960

※「大学、研究機関等」には、高等学校等の教育機関を含む。

※「行政機関等」には、独立行政法人、特殊法人、地方公共団体及びこれらの附属機関を含む。

※「プロバイダ」とは、インターネットに接続する機能を提供する電気通信事業者をいう。

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

注2 ここでいう認知件数とは、不正アクセス被害の届出を受理した場合のほか、余罪として新たな不正アクセス行為の事実を確認した場合、報道を踏まえて事業者等に不正アクセス行為の事実を確認した場合その他関係資料により不正アクセス行為の事実を確認することができた場合において、被疑者が行った犯罪構成要件に該当する行為の数をいう。

注3 特定電子計算機とは、ネットワークに接続されたコンピュータをいい、アクセス管理者とは、特定電子計算機を誰に利用させるかを決定する者をいう。

(3) 認知の端緒

不正アクセス行為の認知件数について、認知の端緒別に内訳を見ると、「警察活動」が最も多く（1,555件）、次いで「利用権者<sup>注4</sup>からの届出」（761件）、「アクセス管理者からの届出」（602件）の順となっている。

図 1 - 2 令和元年における認知の端緒別認知件数

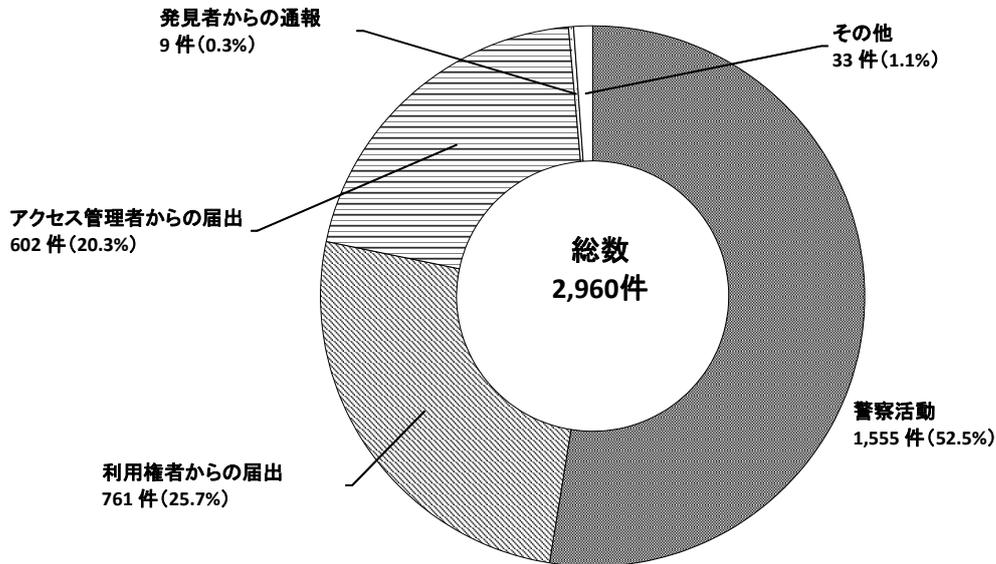


表 1 - 2 過去5年の認知の端緒別認知件数

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

注4 利用権者とは、ネットワークを通じて特定電子計算機を利用することについて、当該特定電子計算機のアクセス管理者の許諾を得た者をいう。例えば、プロバイダからインターネット接続サービスを受けることを認められた会員や企業からLANを利用することを認められた社員が該当する。

(4) 不正アクセス後の行為

不正アクセス行為の認知件数について、不正アクセス後に行われた行為別に内訳を見ると、「インターネットバンキングでの不正送金等」が前年から約5.5倍に増加して最も多く（1,808件）、次いで「インターネットショッピングでの不正購入」（376件）、「メールの盗み見等の情報の不正入手」（329件）の順となっている。

図 1-3 令和元年における不正アクセス後の行為別認知件数

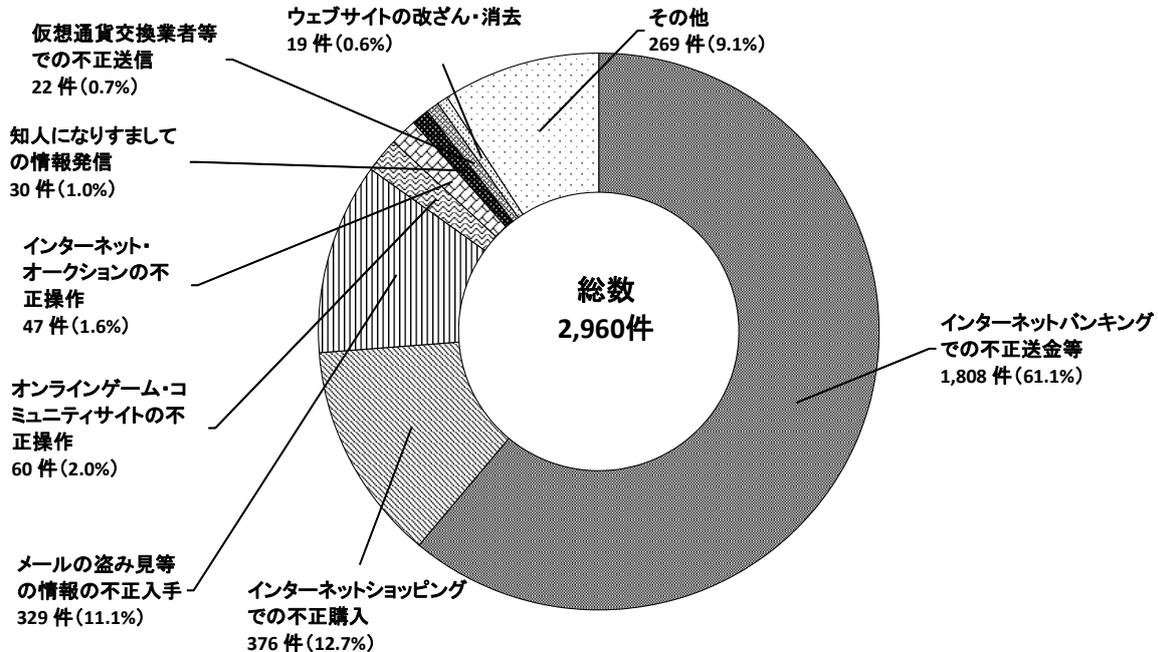


表 1-3 過去5年の不正アクセス後の行為別認知件数

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

※ 平成28年以前は、「仮想通貨交換業者等での不正送信」を分類して集計していない。

## 2 不正アクセス禁止法違反事件の検挙状況

### (1) 検挙件数等

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

検挙件数及び検挙人員について違反行為別に内訳を見ると、「不正アクセス行為」が787件、222人といずれも9割を超えており、他の類型については「識別符号の取得行為<sup>注5</sup>」が5件、4人、「識別符号の提供（助長）行為<sup>注6</sup>」が9件、9人、「識別符号の保管行為<sup>注7</sup>」が13件、7人、「識別符号の不正要求行為<sup>注8</sup>」が2件、1人であった。

表2-1 過去5年の違反行為別検挙件数等

区分		年次	平成27年	平成28年	平成29年	平成30年	令和元年
不正アクセス行為	検挙件数		332	462	599	520	787
	検挙事件数 <sup>注9</sup>		154	175	216	160	218
	検挙人員		154	192	242	164	222
識別符号取得行為	検挙件数		10	6	5	22	5
	検挙事件数		1	3	3	1	4
	検挙人員		1	3	5	2	4
識別符号提供（助長）行為	検挙件数		5	5	9	4	9
	検挙事件数		5	2	6	4	6
	検挙人員		5	3	12	4	9
識別符号保管行為	検挙件数		12	28	31	16	13
	検挙事件数		2	6	2	9	5
	検挙人員		2	6	6	12	7
識別符号不正要求行為	検挙件数		14	1	4	2	2
	検挙事件数		14	1	3	2	1
	検挙人員		14	1	4	2	1
計	検挙件数（件）		373	502	648	564	816
	検挙事件数（事件） （重複3）		173	182	227	170	232 （重複2）
	検挙人員（人） （重複3）		173	200	255	173	234 （重複9）

※ 1事件で複数の区分の行為を検挙した場合又は1人の被疑者を複数の区分の行為で検挙した場合は、それぞれの区分に重複して計上。

注5 不正アクセスの目的で他人の識別符号を取得する行為をいう。

注6 他人の識別符号をアクセス管理者又は利用権者以外の者に正当な理由なく提供する行為をいう。

注7 不正アクセスの目的で他人の識別符号を保管する行為をいう。

注8 アクセス管理者になりすまし、当該アクセス制御機能に係る識別符号の入力を求める行為をいう。例えば、ID・パスワードの入力を求めるフィッシングサイトを公衆が閲覧できる状態に置く行為が該当する。

注9 事件数とは、事件単位ごとに計上した数であり、一連の捜査で複数の件数の犯罪を検挙した場合は1事件と数える。

- (2) 不正アクセス行為の手口別検挙状況  
不正アクセス行為の検挙件数について手口別に内訳を見ると、「識別符号窃用型<sup>注10</sup>」が785件と約99.7%を占めている。

表2-2 過去5年の不正アクセス行為の手口別検挙件数等

区分		年次				
		平成27年	平成28年	平成29年	平成30年	令和元年
識別符号窃用型	検挙件数	331	457	545	502	785
	検挙事件数	153	174	213	155	216
セキュリティ・ホール攻撃型	検挙件数	1	5	54	18	2
	検挙事件数	1	3	5	6	2
計	検挙件数 (件)	332	462	599	520	787
	検挙事件数 (事件)	154	175 (重複)	216 (重複)	160 (重複)	218

※ 1事件で複数の区分の行為を検挙した場合は、それぞれの区分に重複して計上。

注10 アクセス制御されているサーバに、ネットワークを通じて、他人の識別符号を入力して不正に利用する行為（不正アクセス禁止法第2条第4項第1号に該当する行為）をいう。

### 3 検挙した不正アクセス禁止法違反事件の特徴

#### (1) 被疑者等の年齢

検挙した不正アクセス禁止法違反に係る被疑者の年齢は、「20～29歳」が93人で最も多く、次いで「14～19歳」が55人、「30～39歳」が50人の順となっている<sup>注11</sup>。

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<sup>注12</sup>、最年長の者は62歳であった。

図3-1 令和元年における年代別被疑者数

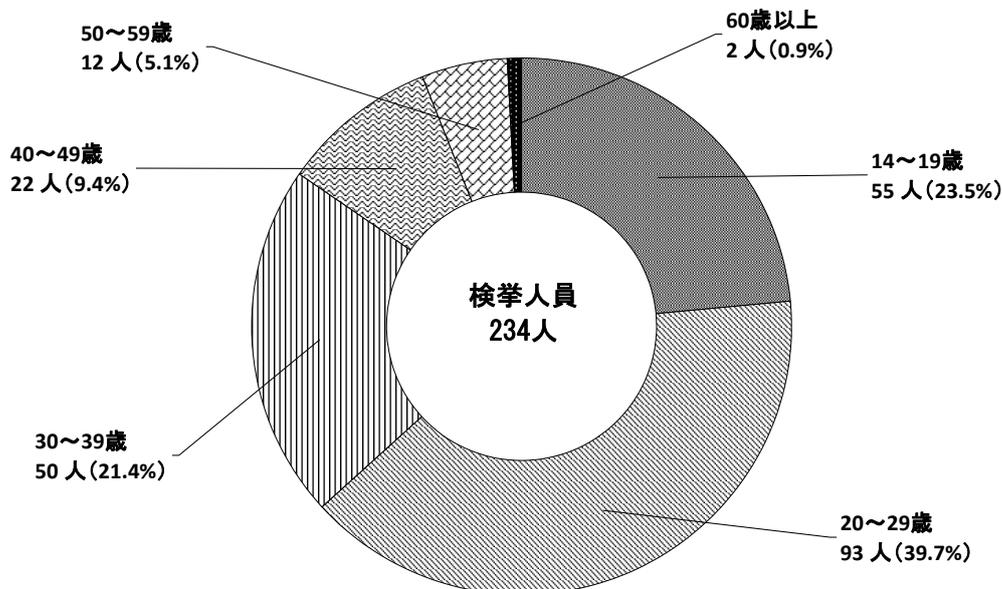


表3-1 過去5年の年代別被疑者数の推移

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

#### (2) 被疑者と利用権者の関係

不正アクセス禁止法違反に係る被疑者と識別符号を窃用された利用権者との関係を見ると、「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(127人)、次いで「交友関係のない他人によるもの」(91人)、「ネットワーク上の知り合いによるもの」(16人)の順となっている。

注11 このほか、不正アクセス禁止法違反により14歳未満の少年6人が触法少年として補導されている(犯罪統計による集計)。

注12 14歳未満の少年であるため、検挙事件及び検挙人員としては計上していない。

(3) 不正アクセス行為の手口

検挙した不正アクセス禁止法違反に係る識別符号窃用型の不正アクセス行為の手口を見ると、「利用権者のパスワードの設定・管理の甘さにつけ込んだもの」が最も多く（310件）、次いで「他人から入手したもの」（182件）となっており、前年と比較するとそれぞれ約1.1倍、14倍となっている。

図3-2 令和元年における不正アクセス行為（識別符号窃用型）に係る手口別検挙件数

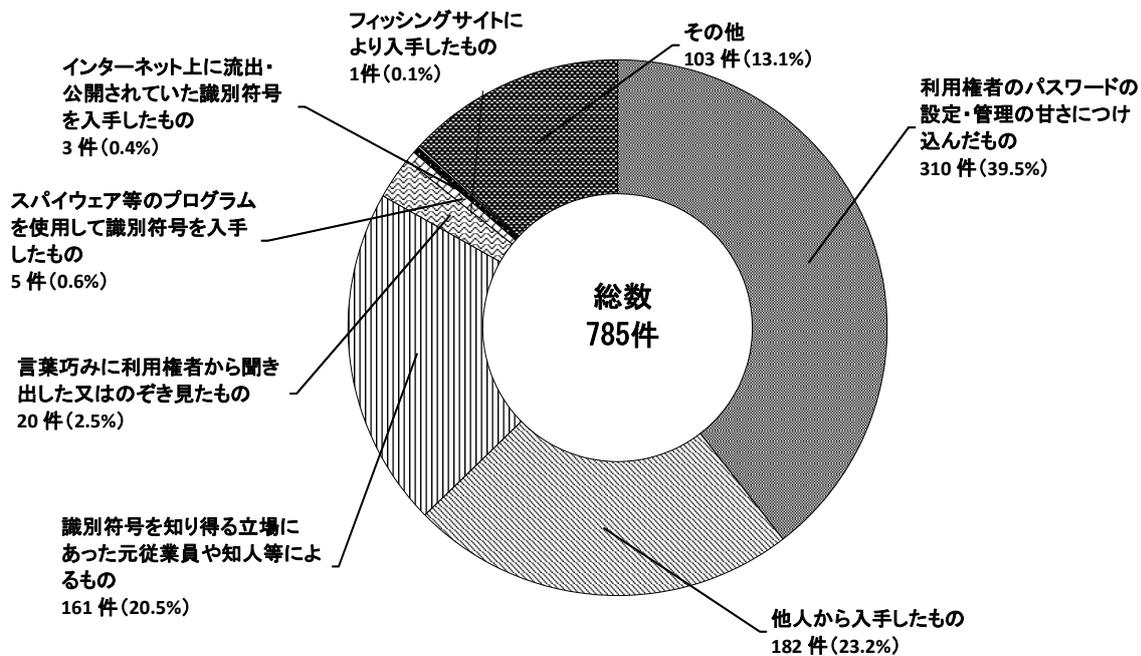


表3-2 過去5年の不正アクセス行為に係る手口別検挙件数

区分	年次	平成27年	平成28年	平成29年	平成30年	令和元年
識別符号窃用型（件）		331	457	545	502	785
利用権者のパスワードの設定・管理の甘さにつけ込んだもの		117	244	230	278	310
他人から入手したもの		13	20	74	13	182
識別符号を知り得る立場にあった元従業員や知人等によるもの		51	61	113	131	161
言葉巧みに利用権者から聞き出した又はのぞき見たもの		46	49	42	17	20
スパイウェア <sup>注13</sup> 等のプログラムを使用して識別符号を入手したもの		15	34	37	0	5
インターネット上に流出・公開されていた識別符号を入手したもの		57	4	0	7	3
フィッシングサイトにより入手したもの		24	3	2	3	1
その他		8	42	47	53	103
セキュリティ・ホール攻撃型（件）		1	5	54	18	2

注13 パソコン内のファイル情報、キーボードの入力情報、表示画面の情報等を取り出して、漏えいさせる機能を持つプログラムをいう。

(4) 不正アクセス行為の動機

検挙した不正アクセス禁止法違反に係る不正アクセス行為の動機を見ると、「不正に経済的利益を得るため」が最も多く（333件）、次いで「顧客データの収集等情報を不正に入手するため」（254件）、「嫌がらせや仕返しのため」（68件）の順となっている。

図3-3 令和元年における不正アクセス行為に係る動機別検挙件数

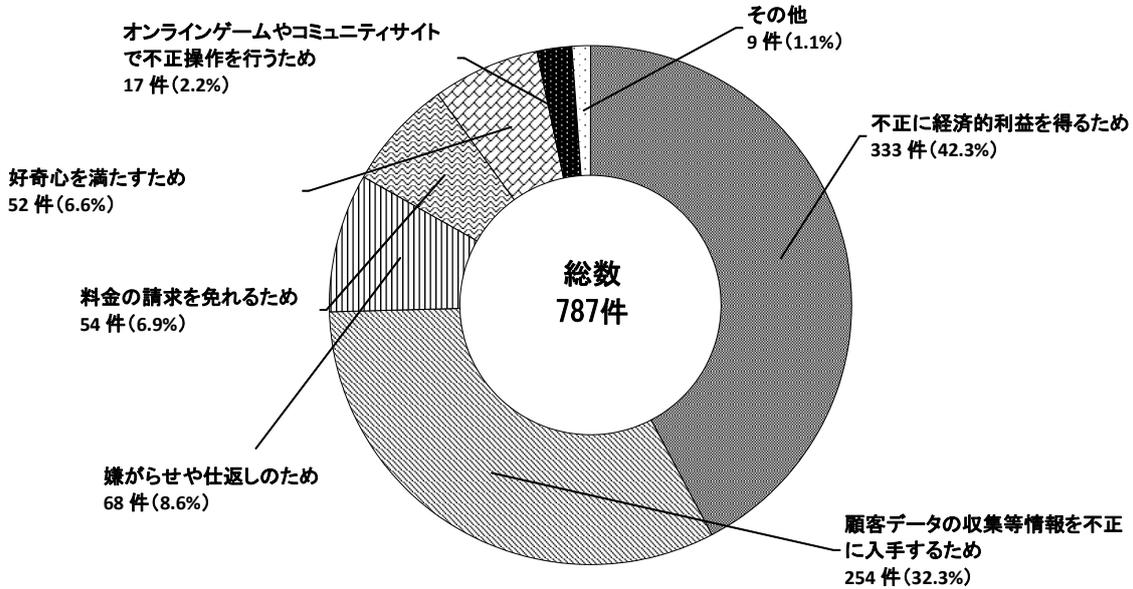


表3-3 過去5年の不正アクセス行為に係る動機別検挙件数

区分	年次				
	平成27年	平成28年	平成29年	平成30年	令和元年
不正に経済的利益を得るため	52	41	93	22	333
顧客データの収集等情報を不正に入手するため	72	70	103	195	254
嫌がらせや仕返しのため	44	44	59	46	68
料金の請求を免れるため	58	25	86	15	54
好奇心を満たすため	76	208	193	103	52
オンラインゲームやコミュニティサイトで不正操作を行うため	28	43	43	101	17
その他	2	31	22	38	9
計（件）	332	462	599	520	787

(5) 不正に利用されたサービス

検挙した不正アクセス禁止法違反に係る識別符号窃用型の不正アクセス行為（785件）について、他人の識別符号を用いて不正に利用されたサービス別の内訳を見ると、「オンラインゲーム・コミュニティサイト」が最も多く（224件）、次いで「社員・会員用等の専用サイト」（151件）となっており、前年と比較すると、それぞれ横ばい、24.5%の減少となっている。

図3-4 令和元年における不正アクセス行為（識別符号窃用型）に係る不正に利用されたサービス別検挙件数

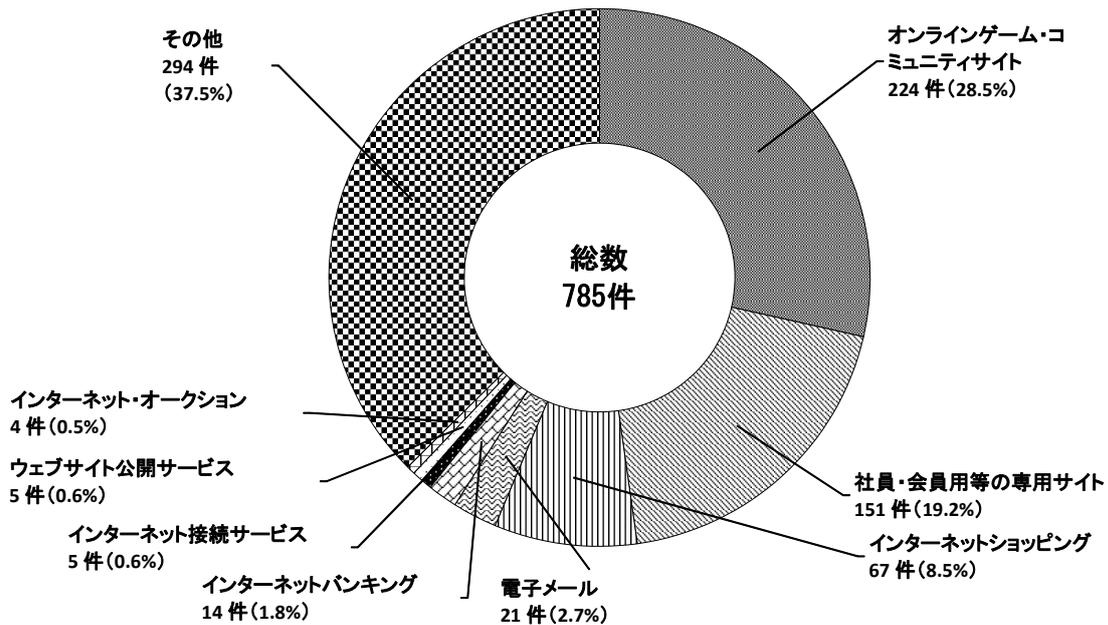


表3-4 過去5年の不正に利用されたサービス別検挙件数

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

#### 4 検挙事例

- (1) 無職の男(62)は、平成30年11月、インターネットサービスプロバイダの会員サイトに対して、他人のID・パスワードを使用して不正アクセスし、パスワード等を変更した。平成31年2月、不正アクセス禁止法違反(不正アクセス行為)と私電磁的記録不正作出・同供用で逮捕した。(栃木)
- (2) 外国人留学生の男(27)は、平成30年9月、大手企業の会員サイトに対して、他人のID・パスワードを使用して不正アクセスし、他人のアカウント保管の換金可能なポイントを自らが作成したアカウントに移動した。平成31年3月、不正アクセス禁止法違反(不正アクセス行為)と電子計算機使用詐欺で逮捕した。(千葉)
- (3) 中国国籍の男(29)は、令和元年7月、不正に取得したID・パスワードを使用して、コード決済システムに不正アクセスし、コンビニエンスストアにおいて、電子タバコカートリッジを騙し取った。同年10月、不正アクセス禁止法違反(不正アクセス行為)と詐欺罪で逮捕した。(熊本)
- (4) 公務員の男(50)は、平成29年1月から平成31年2月までの間、勤務先の同僚のID・パスワードを無断で使用し、公務用サーバに不正アクセスし、同サーバ内のデータを不正に入手した。令和元年9月、不正アクセス禁止法違反(不正アクセス行為)で検挙した。(長崎)
- (5) 会社員の男(31)は、令和元年5月、勤務先の同僚のID・パスワードを無断で使用し、勤務先の福利厚生サイトに不正アクセスした上、同僚のアカウント保管のポイントを使用し、ギフト券を購入した。令和元年11月、不正アクセス禁止法違反(不正アクセス行為)と電子計算機使用詐欺で逮捕した。(静岡)

## 第2 防御上の留意事項

### 1 利用権者の講ずべき措置

#### (1) パスワードの適切な設定・管理

利用権者のパスワードの設定・管理の甘さにつけ込んだ手口が発生していることから、パスワードを設定する場合には、IDと同じものや利用権者の名前、電話番号、誕生日等のパスワードの推測が容易なものを避けるほか、複数のサイトで同じID・パスワードの組合せを使用しないなどの対策を講ずる。また、パスワードを他人に教えないなど、自己のパスワードは適切に管理する。

#### (2) フィッシングに対する注意

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

#### (3) 不正に用いられるプログラムに対する注意

コンピュータにプログラムを不正に感染させ、他人のID・パスワードを不正に取得する事案も発生していることから、心当たりのある企業からの電子メールであっても、正当な電子メールと判断できるまでは添付ファイルを開かないことや、電子メールに記載のリンクをクリックしないことを徹底するとともに、不特定多数が利用するコンピュータではクレジットカード情報等の重要な情報を入力しないことも徹底する。また、不正に用いられるプログラムへの対策（ウイルス対策ソフトの利用のほか、オペレーティングシステムやウイルス対策ソフトを含む各種ソフトウェアのアップデート等）を適切に講ずる。特に、インターネットバンキング、仮想通貨の取引、インターネットショッピング、オンラインゲーム等の利用に際しては、セキュリティ対策ソフトを利用するとともに、ワンタイムパスワード<sup>注14</sup>又は二経路認証<sup>注15</sup>・二要素認証<sup>注16</sup>を導入するなどの金融機関等が推奨するセキュリティ対策を積極的に利用する。

### 2 アクセス管理者の講ずべき措置

#### (1) 運用体制の構築

正規利用権者が通常使用するIPアドレスや時間帯等と異なる不審なログインを早期に検知する体制を構築する。

#### (2) パスワードの適切な設定

利用権者のパスワードの設定・管理の甘さにつけ込んだ不正アクセス行為が発生していることから、文字数や使用文字に条件を付けるなど、容易に推測されるパスワードを設定できないようにするほか、複数のサイトで同じID・パスワードの組合せを使用することの危険性を周知するなどの措置を講ずる。

#### (3) ID・パスワードの適切な管理

元従業員や委託先業者等ID・パスワードを知り得る立場にあった者による不正

注14 インターネットバンキング等における認証用のパスワードであって、認証のたびにそれを構成する文字列が変わるものをいう。これを導入することにより、識別符号を盗まれても次回の利用時に使用できないこととなる。

注15 インターネットバンキング等において、パーソナルコンピュータ（第一経路）で振り込み等の取引データを作成した後、スマートフォン等（第二経路）で承認を行うことで取引を成立させる認証方式をいう。

注16 人の認証に用いられる三つの要素（本人だけが知っていること、本人だけが所有しているもの及び本人自身の特徴）から二つの要素を組み合わせる用いる認証方式をいう。本人だけが知っているID・パスワードによる認証に本人だけが所有するスマートフォンアプリによる認証を追加する場合等がこれに当たる。

アクセス行為が発生していることから、利用権者が特定電子計算機を利用する立場でなくなったときには、当該者に割り当てていたIDを削除したり、パスワードを変更したりするなど、ID・パスワードの適切な管理を徹底する。

(4) フィッシング等への対策

フィッシング等により取得したID・パスワード等を用いて不正アクセス行為を行う事案が発生しているほか、フィッシング等によって不正に取得された可能性があるID・パスワードがインターネット上に流出・公開される事例もあることから、ワンタイムパスワード又は二経路認証・二要素認証の導入等により認証を強化するほか、自らが管理する特定電子計算機に係るフィッシング等の情報を収集し、利用者に注意喚起を行うなどの措置を講ずる。

(5) セキュリティ・ホール攻撃への対応

SQLインジェクション<sup>注17</sup>攻撃、ウェブサーバの脆弱性に対する攻撃等のセキュリティ・ホール攻撃への対策として、定期的にウェブサーバのプログラムを点検してセキュリティ上の脆弱性を解消するとともに、攻撃の兆候を即座に検知するためのシステムを導入するなど、セキュリティ・ホール攻撃に対する監視体制を強化する。

---

注17 SQLというプログラム言語を用いて、企業等が個人情報管理するデータベースを外部から不正に操作する行為をいう。

(参考) 不正アクセス関連行為の関係団体への届出状況について

○ 独立行政法人情報処理推進機構（IPA）に届出のあったコンピュータ不正アクセスの届出状況について

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

令和元年は平成30年と比べて、35件(約64.8%)増加した。

届出のうち実際に被害があったケースにおける被害内容の分類では、「なりすまし」による被害が多く寄せられた。

以下に、種々の切り口で分類した結果を示す。個々の件数には未遂(実際の被害はなかったもの)も含まれる。また、1件の届出にて複数の項目に該当するものがあるため、それぞれの分類での総計件数はこの89件に必ずしも一致しない。

(1) 手口別分類

意図的に行う攻撃行為による分類である。1件の届出について複数の攻撃行為を受けている場合もあるため、届出件数とは一致せず総計は126件(平成30年:73件)となる。

ア 侵入行為に関して

侵入行為に係る攻撃等の届出は59件(平成30年:33件)あった。

(ア) 侵入の事前調査行為

システム情報の調査、稼働サービスの調査、アカウント名の調査等である。

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

(イ) 権限取得行為(侵入行為)

パスワード推測やソフトウェアのバグ等のいわゆるセキュリティホールを利用した攻撃や、システムの設定内容を利用した攻撃等による侵入のための行為である。

23件の届出があり、これらのうち実際に侵入につながったものは16件である。

【主な内容】

パスワード推測:10件

- (ウ) 不正行為の実行及び目的達成後の行為  
侵入その他、何らかの原因により不正行為を実行されたことについては  
39 件の届出があった。

**【主な内容】**

ファイル等の改ざん、破壊等：28 件  
プログラムの作成・設置（インストール）、トロイの木馬等の埋め込み  
等：9 件

イ サービス妨害攻撃

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

ウ その他

その他にはメール不正中継やメールアドレス詐称、正規ユーザになりすま  
してのサービスの不正利用、ソーシャルエンジニアリング等が含まれ、55 件  
（平成 30 年：29 件）の届出があった。

**【主な内容】**

正規ユーザへのなりすまし：21 件  
スパムメール：7 件

(2) 原因別分類

不正アクセスを許した問題点／弱点による分類である。

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

被害原因として「設定の不備（セキュリティ上問題のあるデフォルト設定を  
含む。）」が多いが、これは、サーバ側のアクセス制限を行っていなかった等、  
セキュリティ上問題のあるデフォルト設定の隙を狙った攻撃が多いためであ  
ると推測される。また、原因が不明なケースも依然として少なくはなく、手口  
の巧妙化により原因の特定に至らない事例が多いと推測される。

**【主な要因】**

設定の不備（セキュリティ上問題のあるデフォルト設定を含む。）による  
もの：15 件  
原因不明：15 件  
ID、パスワード管理の不備によると思われるもの：9 件  
古いバージョンの利用や、パッチ・必要なプラグイン等の未導入による  
もの：7 件

### (3) 電算機分類

不正アクセス行為の対象となった機器による分類である（被害の有無は問わない。）。

#### 【主な対象】

WWW サーバ：29 件

メールサーバ：6 件

クライアント：6 件

不明：4 件

※ 1 件の届出で複数の項目に該当するものがある。

### (4) 被害内容分類

89 件の届出を被害内容で分類すると 123 件となるが、そのうち、実際に被害に遭ったケースにおける被害内容による分類である。機器に対する実被害があった件数は 82 件（平成 30 年：47 件）である。

なお、対処に係る工数やサービスの一時停止、代替機の準備等に関する被害は除外している。

#### 【主な被害内容】

データの窃取や盗み見：28 件

オンラインサービスの不正利用：19 件

ファイルの書き換え：8 件

踏み台として悪用：7 件

ホームページ改ざん：6 件

※ 1 件の届出で複数の項目に該当するものがある。

### (5) 対策情報

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

ウェブサイト等のサーバへの不正アクセスを防ぐためには、以下のような対策が必要となる。

システム管理者向け対策 としては、

- ・ ウェブアプリケーションの定期的な脆弱性対策の実施
  - ・ ウェブサーバ上の不要なサービスの停止
- など、ウェブサイトのセキュリティホールを無くしていくことが推奨される。

また、ユーザの対策 としては、

- ・ 他者に推測されにくい複雑なパスワードを設定する
  - ・ パスワードの使いまわしをしない
  - ・ 二段階認証などのセキュリティオプションを積極的に採用する
- など、適切なアカウント管理とリスクへの対策を実施することが推奨される。

下記ページ等を参照し、今一度状況確認・対処されたい。

【システム管理者向け】

「安全なウェブサイトの運用管理に向けての 20 ヶ条  
～セキュリティ対策のチェックポイント～」

<https://www.ipa.go.jp/security/vuln/websitecheck.html>

「安全なウェブサイトの作り方 改訂第 7 版」

<https://www.ipa.go.jp/security/vuln/websecurity.html>

「JVN (Japan Vulnerability Notes)」 ※脆弱性対策情報ポータルサイト

<https://jvn.jp/>

「IPA メールニュース」

<https://www.ipa.go.jp/about/mail/>

【個人ユーザ向け】

「ここからセキュリティ」情報セキュリティ・ポータルサイト

<https://www.ipa.go.jp/security/kokokara/>

「IPA セキュリティセンター・個人ユーザ向けページ」

<https://www.ipa.go.jp/security/personal/index.html>

「MyJVN」(セキュリティ設定チェック、バージョンチェック)

<https://jvndb.jvn.jp/apis/myjvn/>

ウイルス対策を含むセキュリティ関係の情報・対策等については、下記ページを参照のこと。

「IPA セキュリティセンタートップページ」

<https://www.ipa.go.jp/security/index.html>

注1 コンピュータ不正アクセス

システムを利用する者が、その者に与えられた権限によって許された行為以外の行為を、ネットワークを介して意図的に行うこと。

注2 ここに挙げた件数は、コンピュータ不正アクセスの届出を IPA が受理した件であり、不正アクセスやアタック等に関して実際の発生件数や被害件数を直接類推できるような数値ではない。

○ 一般社団法人 JPCERT コーディネーションセンター（以下、JPCERT/CC）に報告があった不正アクセス関連行為の状況について

JPCERT/CC は、国内の情報セキュリティインシデントの被害低減を目的として、広く一般から不正アクセス関連行為を含むコンピュータセキュリティインシデントに関する調整対応依頼を受け付けている。

## 1. 不正アクセス関連行為の特徴および件数

令和元年（平成 31 年 1 月 1 日から令和元年 12 月 31 日までの 1 年間）に JPCERT/CC に報告（調整対応依頼）のあったコンピュータ不正アクセスが対象

報告（調整対応依頼）のあった不正アクセス関連行為（注 1）に係わる報告件数（注 2）は 18,070 件であった。この報告を元にしたインシデント件数（注 3）は 20,303 件であり、インシデントをカテゴリ別に分類すると以下の通りである。

### （1） プローブ、スキャン、その他不審なアクセスに関する報告

防御に成功したアタックや、コンピュータ／サービス／弱点の探査を意図したアクセス、その他の不審なアクセス等、システムのアクセス権において影響を生じないか、無視できるアクセスについて 5,052 件の報告があった。  
[1/1-3/31: 2,165 件、4/1-6/30: 1216 件、7/1-9/30: 927 件、10/1-12/31: 744 件]

### （2） Web サイト改ざん

攻撃者もしくはマルウェアによって、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 1,013 件の報告があった。  
[1/1-3/31: 229 件、4/1-6/30: 256 件、7/1-9/30: 236 件、10/1-12/31: 292 件]

### （3） マルウェアサイト

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 902 件の報告があった。  
[1/1-3/31: 136 件、4/1-6/30: 292 件、7/1-9/30: 269 件、10/1-12/31: 205 件]

### （4） ネットワークやコンピュータの運用を妨害しようとする攻撃

大量のパケットや予期しないデータの送信によって、サイトのネットワークやホストのサービス運用を妨害しようとするアクセスについて 30 件の報告があった。  
[1/1-3/31: 13 件、4/1-6/30: 10 件、7/1-9/30: 1 件、10/1-12/31: 6 件]

#### (5) Web 偽装事案(phishing)

Web のフォームなどから入力された口座番号やキャッシュカードの暗証番号といった個人情報を盗み取る Web 偽装事案について 10,857 件の報告があった。

[1/1-3/31: 1,753 件、4/1-6/30: 1,947 件、7/1-9/30: 3,457 件、10/1-12/31: 3,700 件]

#### (6) 制御システム関連

インターネット経由で攻撃が可能な制御システム等については報告がなかった。

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

#### (7) 標的型攻撃

特定の組織、企業、業種などを標的として、マルウェア感染や情報の窃取などを試みる攻撃について 19 件の報告があった。

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

#### (8) その他

コンピュータウイルス、SPAM メールの受信等について 2,430 件の報告があった。

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

## 2. 防御に関する啓発および対策措置の普及

JPCERT/CC は、日本国内のインターネット利用者に対して、不正アクセス関連行為を防止するための予防措置や、発生した場合の緊急措置などに関する情報を提供し、不正アクセス関連行為への認識の向上や適切な対策を促進するため、以下の文書を公開している(詳細は <http://www.jpccert.or.jp/>参照。)

#### (1) 注意喚起

[新規]

2019 年 1 月	2019 年 1 月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起 2019 年 1 月マイクロソフトセキュリティ更新プログラムに関する
------------	--

	<p>注意喚起</p> <p>Adobe Acrobat および Reader の脆弱性 (APSB19-02) に関する注意喚起</p>
2019 年 2 月	<p>Drupal の脆弱性 (CVE-2019-6340) に関する注意喚起</p> <p>ISC BIND 9 に対する複数の脆弱性 (CVE-2018-5744, CVE-2018-5745, CVE-2019-6465) に関する注意喚起</p> <p>Adobe Acrobat および Reader の脆弱性 (APSB19-13) に関する注意喚起</p> <p>runc の権限昇格の脆弱性 (CVE-2019-5736) に関する注意喚起</p> <p>2019 年 2 月マイクロソフトセキュリティ更新プログラムに関する注意喚起</p> <p>Adobe Flash Player の脆弱性 (APSB19-06) に関する注意喚起</p> <p>Adobe Acrobat および Reader の脆弱性 (APSB19-07) に関する注意喚起</p>
2019 年 3 月	<p>2019 年 3 月マイクロソフトセキュリティ更新プログラムに関する注意喚起</p> <p>Adobe ColdFusion の脆弱性 (APSB19-14) に関する注意喚起</p>
2019 年 4 月	<p>Oracle WebLogic Server の脆弱性 (CVE-2019-2725) に関する注意喚起</p> <p>ISC BIND 9 に対する複数の脆弱性に関する注意喚起</p> <p>Confluence Server および Confluence Data Center における複数の脆弱性に関する注意喚起</p> <p>2019 年 4 月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起</p> <p>2019 年 4 月 Intel 製品の脆弱性に関する注意喚起</p> <p>2019 年 4 月マイクロソフトセキュリティ更新プログラムに関する注意喚起</p> <p>Adobe Flash Player の脆弱性 (APSB19-19) に関する注意喚起</p> <p>Adobe Acrobat および Reader の脆弱性 (APSB19-17) に関する注意喚起</p>
2019 年 5 月	<p>Intel 製品の複数の脆弱性 (INTEL-SA-00213) に関する注意喚起</p> <p>2019 年 5 月マイクロソフトセキュリティ更新プログラムに関する注意喚起</p> <p>Adobe Acrobat および Reader の脆弱性 (APSB19-18) に関する注意喚起</p> <p>Adobe Flash Player の脆弱性 (APSB19-26) に関する注意喚起</p>

2019年6月	Oracle WebLogic Server の脆弱性 (CVE-2019-2729) に関する注意喚起 Firefox の脆弱性 (CVE-2019-11707) に関する注意喚起 2019年6月マイクロソフトセキュリティ更新プログラムに関する注意喚起 Adobe Flash Player の脆弱性 (APSB19-30) に関する注意喚起
2019年7月	2019年7月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起 2019年7月マイクロソフトセキュリティ更新プログラムに関する注意喚起
2019年8月	2019年8月マイクロソフトセキュリティ更新プログラムに関する注意喚起 Adobe Acrobat および Reader の脆弱性 (APSB19-41) に関する注意喚起
2019年9月	Microsoft Internet Explorer の脆弱性 (CVE-2019-1367) に関する注意喚起 2019年9月マイクロソフトセキュリティ更新プログラムに関する注意喚起 Adobe Flash Player の脆弱性 (APSB19-46) に関する注意喚起 ウイルスバスター コーポレートエディションの脆弱性 (CVE-2019-9489) に関する注意喚起 複数の SSL VPN 製品の脆弱性に関する注意喚起
2019年10月	ウイルスバスターコーポレートエディションの脆弱性 (CVE-2019-18187) に関する注意喚起 2019年10月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起 Adobe Acrobat および Reader の脆弱性 (APSB19-49) に関する注意喚起 2019年10月マイクロソフトセキュリティ更新プログラムに関する注意喚起
2019年11月	マルウェア Emotet の感染に関する注意喚起 ISC BIND 9 の脆弱性に関する注意喚起 2019年11月マイクロソフトセキュリティ更新プログラムに関する注意喚起
2019年12月	2019年12月マイクロソフトセキュリティ更新プログラムに関する注意喚起

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

## (2) 活動概要 (報告状況等の公表)

発行日：2019-01-16 [ 2018 年 10 月 1 日 ~ 2018 年 12 月 31 日]

発行日：2019-04-11 [ 2019 年 1 月 1 日 ~ 2019 年 3 月 31 日]

発行日：2019-07-11 [ 2019 年 4 月 1 日 ~ 2019 年 6 月 30 日]

発行日：2019-10-17 [ 2019 年 7 月 1 日 ~ 2019 年 9 月 30 日]

## (3) JPCERT/CC レポート

[発行件数] 50 件

[取り扱ったセキュリティ関連情報数] 323 件

注1 不正アクセス関連行為とは、コンピュータやネットワークのセキュリティを侵害する人為的な行為で、意図的(または、偶発的)に発生する全ての事象が対象になる。

注2 ここにあげた件数は、JPCERT/CC が受け付けた報告の件数である。実際のアタックの発生件数や、被害件数を類推できるような数値ではない。また類型ごとの実際の発生比率を示すものでもない。一定以上の期間に渡るアクセスの要約レポートも含まれるため、アクセスの回数と報告件数も一般に対応しない。報告元には、国内外のサイトが含まれる。

注3 「インシデント件数」は、各報告に含まれるインシデント件数の合計を示す。ただし、1つのインシデントに関して複数件の報告がよせられた場合は、1件のインシデントとして扱う。

## 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
- Web媒介型攻撃対策技術の実用化に向けた研究開発
- 欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発
- サイバー攻撃ハイブリッド分析実現に向けたセキュリティ情報自動分析基盤技術の研究開発

### 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令和元年12月9日から令和2年1月24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が、その結果、提案はなかった。

#### (2) 調査

警察庁が令和元年9月に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（13大学、18件）

東京理科大学（2件）  
福山大学  
島根大学  
名古屋大学  
城西大学  
佐賀大学（3件）  
東京電機大学  
崇城大学  
立命館  
お茶の水女子大学  
北九州市立大学  
広島大学（3件）  
東北工業大学

#### イ 企業（3社、4件）

トビラシステムズ株式会社（2件）  
株式会社FFRI  
株式会社アズジェント

また、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、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314校、企業1,336社の計1,650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)

<b>対象技術</b>	インシデント分析技術
<b>テーマ名</b>	サイバーセキュリティ技術の研究開発
<b>開発年度</b>	平成18年度～
<b>実施主体</b>	国立研究開発法人情報通信研究機構
<b>法人番号</b>	7012405000492
<b>背景、目的</b>	<p>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。</p>
<b>研究開発状況（概要）</b>	<p>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。</p>
<b>詳細の入手方法（関連部署名及びその連絡先）</b>	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
<b>将来の方向性</b>	<p>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。</p>

<b>対象技術</b>	インシデント分析技術
<b>テーマ名</b>	Web媒介型攻撃対策技術の実用化に向けた研究開発
<b>開発年度</b>	平成28年度～平成32年度
<b>実施主体</b>	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）
<b>法人番号</b>	5030001055903（KDDI総合研究所）、6020005004971（横浜国立大学）
<b>背景、目的</b>	<p>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。</p> <p>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）ポイズニング」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。</p> <p>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。</p>
<b>研究開発状況（概要）</b>	<p>平成28年度から以下の研究開発を開始。平成30年度に行った中間評価の結果、平成32年度までの延長を決定。</p> <ul style="list-style-type: none"> <li>（1） 新型ブラウザセンサの研究開発</li> <li>（2） 新型観測機構の研究開発</li> <li>（3） 新型攻撃情報分析基盤の研究開発</li> <li>（4） Web媒介型攻撃対策技術大規模・長期実証実験</li> </ul>
<b>詳細の入手方法（関連部署名及びその連絡先）</b>	<p>国立研究開発法人情報通信研究機構 インノベーション推進部門 委託研究推進室  (<a href="https://www.nict.go.jp/collabo/commission/k_190.html">https://www.nict.go.jp/collabo/commission/k_190.html</a>)  電話 042-327-6011</p>
<b>将来の方向性</b>	<p>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。</p>

<b>対象技術</b>	侵入検知・防御技術、ぜい弱性対策技術
<b>テーマ名</b>	欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発
<b>開発年度</b>	平成30年度～平成33年度
<b>実施主体</b>	東日本電信電話株式会社、学校法人慶應義塾他（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）
<b>法人番号</b>	8011101028104(東日本電信電話株式会社)、4010405001654（学校法人慶應義塾）他
<b>背景、目的</b>	<p>本研究開発は、欧州との連携により研究開発の促進が期待できる領域について、欧州委員会（EC: European Commission）と連携して共同で実施するプログラム。</p> <p>ハイパーコネクテッド社会の実現に向けて、実践的なサイバーセキュリティ技術の研究開発は不可欠である。そのため、セキュリティ、IoT、クラウド及びビッグデータを組み合わせた先端技術の研究開発及び実証を通じ、世界規模で有効かつ実効性のあるサイバーセキュリティ基盤技術の構築を目指す。</p>
<b>研究開発状況（概要）</b>	<p>平成30年度から研究開発を開始。</p> <p>具体的には、「新たな脅威への機敏な対応」、「脆弱性自動検出/自動修復」、「セキュリティツールのオープンソース化」、「IoTセキュリティ」、「クラウドセキュリティ」、「データセキュリティ」、「プライバシー保護」、「データ匿名化」、「IoT/クラウドに関するブロックチェーン」、「重要インフラ保護」、「クロスボーダ・アプリケーション」に関わる研究開発及び実証を行う。</p>
<b>詳細の入手方法（関連部署名及びその連絡先）</b>	<p>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  (<a href="https://www.nict.go.jp/collabo/commission/k_195.html">https://www.nict.go.jp/collabo/commission/k_195.html</a>)  電話 042-327-6011</p>
<b>将来の方向性</b>	<p>国際標準化を睨んだ研究開発力の強化や国際実証環境の構築を軸とした共同研究開発に取り組むことにより、情報通信基盤の共通化を通じた豊かな社会への貢献に資する。</p>

<b>対象技術</b>	インシデント分析技術
<b>テーマ名</b>	サイバー攻撃ハイブリッド分析実現に向けたセキュリティ情報自動分析基盤技術の研究開発
<b>開発年度</b>	令和元年度～令和2年度
<b>実施主体</b>	国立大学法人九州大学、学校法人早稲田大学 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）
<b>法人番号</b>	3290005003743（国立大学法人九州大学）、5011105000953（学校法人早稲田大学） 他
<b>背景、目的</b>	<p>マルウェアへの感染は世界的な問題であり、政府、重要インフラなどの組織に対する脅威は増加の一途を辿っている状況であるが、感染活動の早期把握やそのマルウェアに関する情報の関連組織間での共有ができていない。</p> <p>この問題の解決には、セキュリティインシデント発生の可能性をより早く検知し、それを分析するための関連情報を自動的に生成し、関連付け、そのインシデントのもととなったマルウェアや脆弱性を分析する必要がある。これらのタスクは大量のデータを分析することが求められるため、人手による分析は非現実的である一方で、コンピュータによる自動処理の効果が大きく期待できる領域である。また、これらの分析は単一の分析にて完結するものではなく、例えばライブネットトラフィック分析やダークネットトラフィック分析、マルウェア分析、脆弱性分析、Web情報分析など、様々な分析結果を総合的に判断するハイブリッド分析が求められる。そこで本研究では、国立研究開発法人情報通信研究機構が開発中のマルウェア活動の活性化を自動的に検知する技術と連携し、その検知したイベントに関連するマルウェア・脆弱性・脅威情報などを実時間で精緻に提供することで、より有用性の高いセキュリティ情報自動分析基盤技術の確立を目指す。</p>
<b>研究開発状況（概要）</b>	<p>令和元年度から以下の研究開発を開始。</p> <p>(1) サイバー攻撃インフラ情報の収集と分析、(2) 実時間で実現可能な大規模かつ構造的なマルウェア分析、(3) インテリジェンス情報の生成と分析について</p>
<b>詳細の入手方法（関連部署名及びその連絡先）</b>	<p>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  (<a href="https://www.nict.go.jp/collabo/commission/k_21601.html">https://www.nict.go.jp/collabo/commission/k_21601.html</a>)  電話 042-327-6011</p>
<b>将来の方向性</b>	<p>感染活動を自動的に検知し、マルウェアに関する情報と共に自動的に警告を提供可能となる。安心・安全な国際的なサイバー社会の構築・運営に大きく貢献する。</p>

(別添2)

ア 大学

企業・大学名	東京理科大学理工学部
代表者名	井手本康
所在地	〒278-8510 千葉県野田市山崎2641
窓口部署名	理工学事務課
電話番号	04-7122-9728
ホームページのURL	https://st.tus.ac.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： ホームページ掲載内容改ざん 検知及び自動修正システム	ホームページで公開される内容が改ざんされることで一番危険なことは、「改ざんされた情報が一般大衆の視線にさらされてしまうこと」です。本システムは不正侵入を即時検知すると同時に、不正改ざんされた情報をすぐに自動修正することで、誤った情報の流布を阻止することを目的としています。現在、新潟大学理学部のホームページにおいて、私の作製した本システムが実用化されています。(但し、もう、新潟大のHPが外部サービスに委託された可能性もあります。)
開発元(メーカー名等)： シスコ・ネットワーキング・ アカデミー	
開発国： 日本	
価格： シスコネットワーキングアカ デミー会員限定無償配布で す。	
発売時期： 平成25年4月1日～	
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	東京理科大学理工学部
代表者名	井手本康
所在地	〒278-8510 千葉県野田市山崎2641
窓口部署名	理工学事務課
電話番号	04-7122-9728
関連部門名	理工学部情報科学科・東京理科大学CCNA講座
ホームページのURL	<a href="https://st.tus.ac.jp">https://st.tus.ac.jp</a>
研究説明のURL	シスコシステムズ及びシスコネットワークングアカデミーの担当者達による守秘義務が求められています
対象技術	研究開発状況
研究開発名称： クラウド化されたハニーポットシステム	<ul style="list-style-type: none"> <li>・サイバー犯罪対策は大きく「防御」と「犯人特定」の2種類に大別されます。しかし、現在のセキュリティ対策は防御のみが中心で、消極的対策である感じが致します。</li> <li>・東京オリンピック2020では、全てのネットワークシステムを、シスコシステムズが管理することを総務省が決定しており、現在、前回のリオデジャネイロオリンピックにおけるサイバー攻撃のデータを分析し、東京オリンピックにおける防御ガイドラインを作成しています。</li> <li>・本システムは、通常、単体でおとり捜査目的で設定されるハニーポットをネットワークレベルで実装することで、仮想化技術と並用し、クラウドレベルでの犯罪者検知及び犯罪者が用いた技術の抜きとりに使用されています。</li> </ul>
研究開発国： 日本	
研究開発時期： 平成31年4月1日～	

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	福山大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	福山大学工学部情報工学科
ホームページのURL	
研究説明のURL	<a href="http://www.yama-lab.org/~yamanoue/wiki/index.php?BotCapturingNet">http://www.yama-lab.org/~yamanoue/wiki/index.php?BotCapturingNet</a>
対象技術	研究開発状況
研究開発名称： 遠隔操作ウイルス包囲網	○ Gameover Zeus のようなウイルスを想定し、その通信をまねたプログラムを作成し、そのプログラムの検知をある程度できることを示している。スピードが遅いため、その部分の改良を行っている。
研究開発国： 日本	
研究開発時期： 平成24年4月～	

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	国立大学法人島根大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	学術研究院理工学系
ホームページのURL	
研究説明のURL	<a href="https://www.staffsearch.shimane-u.ac.jp/kenkyu/search/f9744d5cdf8b80135d91ac82c25fb108/detail?page=research">https://www.staffsearch.shimane-u.ac.jp/kenkyu/search/f9744d5cdf8b80135d91ac82c25fb108/detail?page=research</a>
対象技術	研究開発状況
研究開発名称： 耐量子計算機暗号の多項式数 理における安全性評価手法の 確立  研究開発国： 日本  研究開発時期： 平成31年4月1日～令和5年3月 31日	

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	国立大学法人名古屋大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報基盤センター 情報基盤ネットワーク部門
ホームページのURL	
研究説明のURL	<a href="https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/network.html">https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/network.html</a>
対象技術	研究開発状況
研究開発名称： （特になし）	
研究開発国： 日本	
研究開発時期： 継続的	

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	学校法人城西大学
代表者名	上原明
所在地	〒102-0094 東京都千代田区紀尾井町3番26号
窓口部署名	城西大学理学部事務室
電話番号	049-271-7728
関連部門名	とくに無し(現段階では個人による研究)。
ホームページのURL	<a href="http://www.josai.ac.jp">http://www.josai.ac.jp</a>
研究説明のURL	とくに無し。
対象技術	研究開発状況
研究開発名称： AIと情報セキュリティに関する研究	AI とりわけ深層学習理論と情報セキュリティの融合領域に焦点を当て研究している。まだ研究の初期段階であり、様々な知見を蓄積して、取り組むべき重要な問題(テーマ)を絞り込んでいる。
研究開発国： 日本	
研究開発時期： とくに決めていない。	

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	佐賀大学理工学部
代表者名	理工学部長 渡孝則
所在地	〒840-8502 佐賀市本庄町1
窓口部署名	
電話番号	
関連部門名	佐賀大学理工学部 廣友研究室
ホームページのURL	
研究説明のURL	
対象技術	研究開発状況
研究開発名称： IoT機器向き軽量暗号・認証方式	認証方式を開発した。仕様は論文として発表している。暗号方式への拡張を行っている。
研究開発国： 日本	
研究開発時期： 平成28年4月1日～	

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	佐賀大学理工学部
代表者名	理工学部長 渡孝則
所在地	〒840-8502 佐賀市本庄町1
窓口部署名	
電話番号	
関連部門名	佐賀大学理工学部 廣友研究室
ホームページのURL	
研究説明のURL	
対象技術	研究開発状況
研究開発名称： IoT機器のためのハニーポット	現在、IoT機器向けハニーポットを開発している。プロトタイプは作成できている。
研究開発国：	
研究開発時期： 平成29年8月1日～	

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	佐賀大学理工学部
代表者名	理工学部長 渡孝則
所在地	〒840-8502 佐賀市本庄町1
窓口部署名	
電話番号	
関連部門名	佐賀大学理工学部 廣友研究室
ホームページのURL	
研究説明のURL	
対象技術	研究開発状況
研究開発名称： ブロックチェーンを用いたログ保存システム	ブロックチェーンを用いてログを保存する要素技術を開発している。
研究開発国： 日本	
研究開発時期： 平成30年10月1日～	

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	東京電機大学 総合研究所 サイバー・セキュリティ研究所
代表者名	
所在地	〒120-8551 東京都足立区千住旭町5番
窓口部署名	
電話番号	
関連部門名	東京電機大学 総合研究所 サイバー・セキュリティ研究所
ホームページのURL	<a href="http://www.dendai.ac.jp/crc/">http://www.dendai.ac.jp/crc/</a>
研究説明のURL	<a href="http://www.lab.ine.aj.dendai.ac.jp/wordpress/">http://www.lab.ine.aj.dendai.ac.jp/wordpress/</a>
対象技術	研究開発状況
研究開発名称： セキュア電子メール、秘密映像伝送、クラウドデータ保管	秘密電子メール、秘密映像伝送技術ならびにクラウドを活用したデータの安全分散保管技術に関しては、プロトタイプソフトウェアを試作し、技術展示が出来るレベルに達している。
研究開発国： 日本	
研究開発時期： 平成19年3月6日～令和2年12月31日	

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	崇城大学
代表者名	理事長・学長 中山峰男
所在地	〒860-0082 熊本県熊本市西区池田4-22-1
窓口部署名	総合企画課
電話番号	096-326-3791
関連部門名	崇城大学 情報学部 情報学科
ホームページのURL	<a href="https://www.sojo-u.ac.jp">https://www.sojo-u.ac.jp</a>
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 軽量カオス暗号の開発	カオスに基づく暗号用非線形変換関数を設計中である。
研究開発国： 日本	
研究開発時期： 平成27年4月1日～	

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	学校法人立命館
代表者名	森島朋三
所在地	〒604-8520 京都市中京区西ノ京栞尾町8番地
窓口部署名	
電話番号	
関連部門名	情報理工学部
ホームページのURL	www.ritsumeai.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 標的型攻撃における攻撃者特定	方式検討を終了し、プロトタイプ実装中。
研究開発国： JP	
研究開発時期： 平成30年4月1日～	

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	国立大学法人お茶の水女子大学
代表者名	学長 室伏きみ子
所在地	〒112-8610 東京都文京区大塚2-1-1
窓口部署名	研究協力課
電話番号	03-5978-5503
関連部門名	お茶の水女子大学 小口研究室
ホームページのURL	<a href="http://www.ocha.ac.jp/">http://www.ocha.ac.jp/</a>
研究説明のURL	<a href="https://www.yama.info.waseda.ac.jp/crest/">https://www.yama.info.waseda.ac.jp/crest/</a>
対象技術	研究開発状況
研究開発名称： JST CREST ビッグデータ統合 利用のためのセキュアなコン テンツ共有・流通基盤の構築	
研究開発国： 日本	
研究開発時期： 平成27年10月1日～令和3年3月 31日	

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	北九州市立大学国際環境工学部
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	北九州市立大学国際環境工学部情報システム工学科
ホームページのURL	
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 携帯端末を対象とした生体認証の信頼性に関する研究	本研究開発は、スマートフォンやタブレットPCなどの携帯端末において、個人の身体的特徴あるいは行動的特徴に基づき本人確認を行う生体認証システムの信頼性対策技術を確立することを目的とし、利用環境の変化に対する高い頑健性、生体情報の保護機能の具備、リソースに制約のある環境でのユーザの利便性やシステムの信頼性の維持の三点を柱とする従来にはない携帯端末に適した生体認証システムの実現を目指している。これまでの研究開発において、①認証システム自身がその場に適した認証方式を適応的に選択するという新たなコンセプトに基づくコンテキストウェアナスなマルチファクタ認証システムの提案、②生体情報を保護するテンプレート保護技術に必要な不可欠となる携帯端末から取得可能な筆記情報と音声を用いた生体ビット列生成アルゴリズムの提案、③プロセッサの性能やバッテリー、メモリの容量など使用可能なリソースに制約のある携帯端末での利用を想定した利便性・安全性・リソースのバランスを考慮したユーザ認証アルゴリズムの提案をそれぞれ行い、実際の利用場面を想定したシミュレーション実験に基づき提案方式の有効性を明らかにしている。今後は、開発した生体認証システムの携帯端末への実装に向けて、評価環境を実験室からフィールドに移し、実際の利用環境に近い条件下で当該システムの性能評価を実施する予定である。
研究開発国： 日本	
研究開発時期： 平成28年4月1日～令和2年3月31日	

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	公立大学法人県立広島大学
代表者名	中村健一
所在地	〒734-8558 広島市南区宇品東1-1-71
窓口部署名	地域連携センター
電話番号	082-251-9534
関連部門名	経営情報学科
ホームページのURL	<a href="http://www.pu-hiroshima.ac.jp/">http://www.pu-hiroshima.ac.jp/</a>
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 複数のセキュリティソフトウェアをオールインワン方式で組み込んだ教育用マイクロサーバの開発	大学および大学院の演習で利用することを想定し、オープンソースのセキュリティソフトウェアを複数組み合わせ、マイクロサーバ上で様々な機能を適宜切り替えて利用できるようにシステムを構築している。サーバ起動時に簡単に「ルータとして動作」、「ファイアウォール(IPS)として動作」といった切り替えができるようなシステムになっている
研究開発国： 日本	
研究開発時期： 平成22年4月～	

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	公立大学法人県立広島大学
代表者名	中村健一
所在地	〒734-8558 広島市南区宇品東1-1-71
窓口部署名	地域連携センター
電話番号	082-251-9534
関連部門名	経営情報学科
ホームページのURL	<a href="http://www.pu-hiroshima.ac.jp/">http://www.pu-hiroshima.ac.jp/</a>
研究説明のURL	
対象技術	研究開発状況
研究開発名称： コンテンツ指向型ネットワークにおけるキャッシュ改ざん対策	現在のIPネットワークとは異なるアーキテクチャである「コンテンツ指向型ネットワーク」において通信を阻害するために行われる攻撃であるキャッシュ改ざんを検知し、拡散を抑止する手法について検討・提案を行っている
研究開発国： 日本	
研究開発時期： 平成29年4月～	

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	公立大学法人県立広島大学
代表者名	中村健一
所在地	〒734-8558 広島市南区宇品東1-1-71
窓口部署名	地域連携センター
電話番号	082-251-9534
関連部門名	経営情報学科
ホームページのURL	<a href="http://www.pu-hiroshima.ac.jp/">http://www.pu-hiroshima.ac.jp/</a>
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 無線APの帯域不正占有対策	公共無線LANのAPの利用において、不正に帯域を専有しようとする行為である「inflated ACK-NAV」に対する対策手法の検討・提案を行っている
研究開発国： 日本	
研究開発時期： 平成27年4月～	

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	学校法人東北工業大学
代表者名	樋口龍雄
所在地	〒982-8577 宮城県仙台市太白区八木山香澄町35番1号
窓口部署名	情報サービスセンター
電話番号	022-305-3896
関連部門名	工学部 情報通信工学科 角田研究室
ホームページのURL	<a href="https://www.tohtech.ac.jp/">https://www.tohtech.ac.jp/</a>
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 人間社会のセキュリティ構造 を模倣したIoT向け運用モデル の開発	基本要素のモデル化と基本要件の分析が完了し、インターネット標準のネットワーク管理技術を活用した概念実証のためのプロトタイプ実装を通じて提案の基本的実現性を確認している。現在は、プロトタイプ実装の改良による通信効率の改善などを図るとともに、様々なネットワーク管理技術を活用したプロトタイプ実装を開発し実用性に関する検討を進めている。
研究開発国： 日本	
研究開発時期： 平成27年4月～	

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	トビラシステムズ株式会社
代表者名	明田篤
所在地	〒460-0003 愛知県名古屋市中区錦2丁目5-12 パシフィックスクエア名古屋錦3F
窓口部署名	
電話番号	050-5533-3720
ホームページのURL	http://tobila.com
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： 迷惑電話フィルタ	契約者の利用情報、警察・自治体からの提供情報、自社で独自に収集した情報を元に独自のアルゴリズムを利用して作成された迷惑電話番号情報を用いて、迷惑な電話をフィルタリングします。
開発元(メーカー名等)： トビラシステムズ株式会社	
開発国： 日本	
価格：	
発売時期： 平成23年6月～	
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	トビラシステムズ株式会社
代表者名	明田篤
所在地	〒460-0003 愛知県名古屋市中区錦2丁目5-12 パシフィックスクエア名古屋錦3F
窓口部署名	
電話番号	050-5533-3720
ホームページのURL	http://tobila.com
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： 迷惑メッセージフィルタ	<p>当社独自のアルゴリズムにより収集・分析した迷惑メールデータベースを活用し、詐欺につながるテキスト情報を含むメールやSMSをフィルタするサービス。迷惑メールデータベースは、利用者に届くメールやSMS情報を収集・分析し、迷惑URLとして出現頻度の高いURLや、迷惑メールとしての特徴を持つ本文情報から、独自のアルゴリズムにより危険な疑いのあるURL情報等をパターン抽出し、それらの情報について社内調査を行った上で構築している。</p>
開発元(メーカー名等)： トビラシステムズ株式会社	
開発国： 日本	
価格：	
発売時期： 平成29年9月21日～	
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FFRI
代表者名	鵜飼裕司
所在地	〒150-0013 東京都渋谷区恵比寿1-18-18 東急不動産恵比寿ビル4F
窓口部署名	総務部
電話番号	03-6277-1811
ホームページのURL	<a href="https://www.ffri.jp/">https://www.ffri.jp/</a>
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： FFRI yarai	<p>旧来のセキュリティ対策では防御できない標的型攻撃など、未知の脅威に対しても効果を発揮する次世代エンドポイントセキュリティ。</p> <p>&lt;特徴&gt;</p> <ul style="list-style-type: none"> <li>・ 0-day攻撃や未知のマルウェアなど、未知の脅威にも効果を発揮</li> <li>・ パターンファイルに依存しない独自の5つの検知エンジンを搭載</li> <li>・ 純国産技術による日本発の次世代エンドポイントセキュリティ</li> <li>・ 「防御」を重視し、被害発生・事後対応コストを最小化</li> <li>・ 他社製品と同時使用が可能で、多重防御環境を実現</li> <li>・ 豊富な防御実績と導入実績の一部を公開</li> <li>・ 侵入した脅威の調査・レポーティング・除去を行うEDR機能も追加費用無しで利用可能</li> </ul>
開発元(メーカー名等)： 株式会社FFRI	
開発国： 日本	
価格： 3~9,000円(ボリュームライセンス)	
発売時期： 平成21年5月~	
出荷数： 2019年6月時点で約74万3千件の契約あり※サブスクリプション契約のため出荷数がありません	

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	株式会社アズジェント
代表者名	杉本隆洋(代表取締役社長)
所在地	〒104-0044 東京都中央区明石町6番4号 ニチレイ明石ビル
窓口部署名	セキュリティ・プラス ラボ
電話番号	03-6853-7406
関連部門名	セキュリティ・プラス本部
ホームページのURL	<a href="https://www.asgent.co.jp/">https://www.asgent.co.jp/</a>
研究説明のURL	<a href="https://www.asgent.co.jp/press/releases/2014/20140117-000373.html">https://www.asgent.co.jp/press/releases/2014/20140117-000373.html</a>
対象技術	研究開発状況
研究開発名称： 不正アクセスの経路及び手法 に関する調査研究	セキュリティプラスラボ設立以来、世界中で横行する脅威の実態やその攻撃手法、またそれらの脅威からクラウド環境やモバイルデバイスを含めた情報資源を守るための対策技術の研究はもとより、国内外の有識者や組織との積極的な連携を図ることにより、技術だけでは守ることのできない「ソーシャルエンジニアリング」のような領域まで踏み込んだ広義での「セキュリティ」に関する調査、研究を継続して行っています。また、その調査・研究成果は講演活動、レポート、トレーニング等を通じて市場に発信しています。
研究開発国： 日本	
研究開発時期： 平成26年4月1日～継続中	

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	