不正アクセス行為の発生状況

第１　令和２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

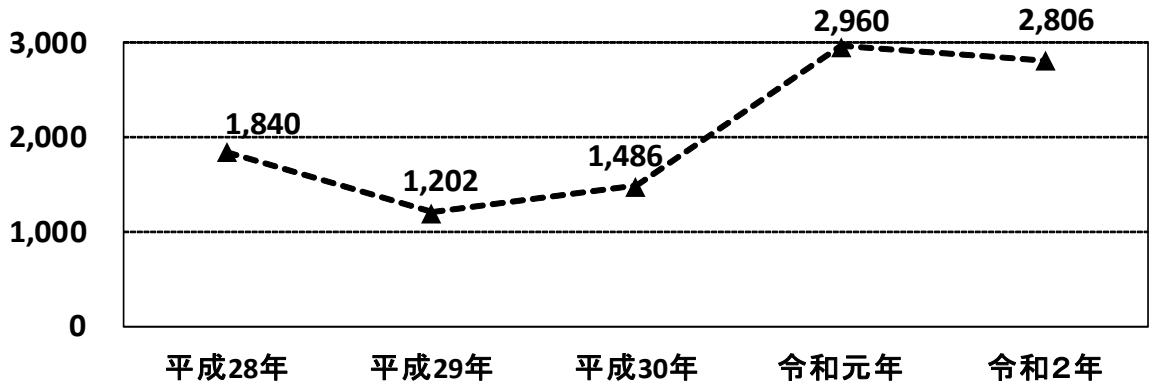
令和２年に都道府県警察から警察庁に報告がなされた不正アクセス行為の認知・検挙状況等は次のとおりである。

１　不正アクセス行為の認知状況

(1)　認知件数

令和２年における不正アクセス行為の認知件数[注1]は2,806件であり、前年（令和元年[注2]）と比べ、154件（約5.2%）減少した。

（件）　図１－１　不正アクセス行為の認知件数の推移（過去５年）



(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別の内訳

令和２年における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3]別に内訳を見ると、「一般企業」が最も多い（2,703件）。

表１－１　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(過去５年)

区分＼年次	平成28年	平成29年	平成30年	令和元年	令和２年
一般企業	1,823	1,177	1,314	2,855	2,703
行政機関等	5	9	6	90	84
大学、研究機関等	2	5	161	3	11
プロバイダ	6	6	4	6	5
その他	4	5	1	6	3
計	1,840	1,202	1,486	2,960	2,806

※「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。
※「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　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て確認した事実のほか、余罪として新たに確認した不正アクセス行為の事実、報道を踏まえて事業者等から確認した不正アクセス行為の事実その他関係資料により確認した不正アクセス行為の事実中、犯罪構成要件に該当する被疑者の行為の数をいう。

注2　令和元年の各種数値については、平成31年１月から４月までの数を含む。

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)　認知の端緒別の内訳

令和２年における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（1,608件）、次いで「アクセス管理者からの届出」（614件）、「利用権者[注4]からの届出」（567件）の順となっている。

図１－２　令和２年における端緒別認知件数

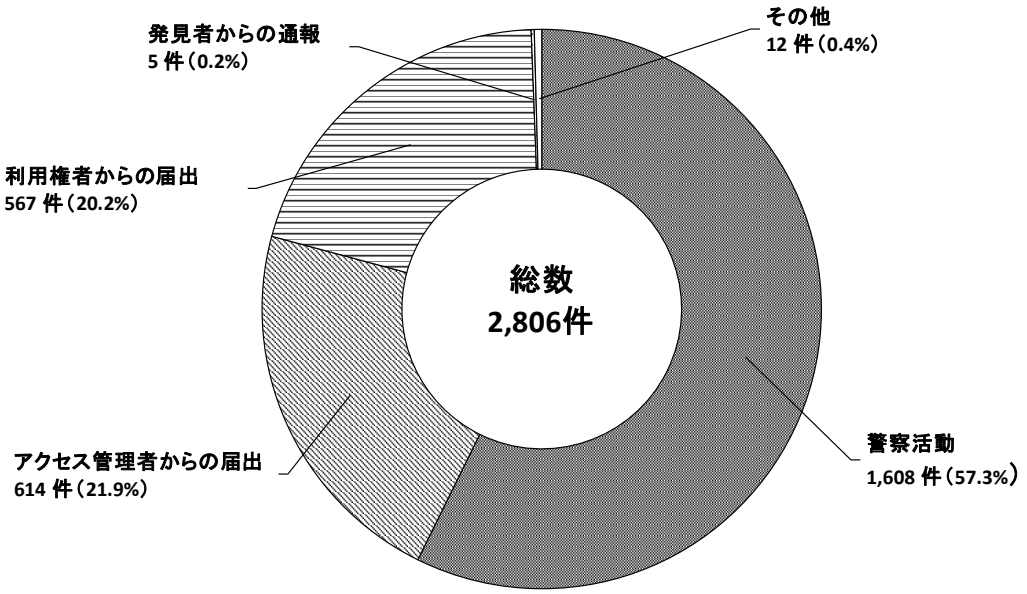


表１－２　端緒別認知件数（過去５年）

区分＼年次	平成28年	平成29年	平成30年	令和元年	令和２年
警察活動	511	283	269	1,555	1,608
アクセス管理者からの届出	828	255	345	602	614
利用権者からの届出	495	655	852	761	567
発見者からの通報	5	6	16	9	5
その他	1	3	4	33	12
計	1,840	1,202	1,486	2,960	2,806

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。

(4)　不正アクセス後の行為別の内訳

令和２年における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」が最も多く（1,847件）、次いで「メールの盗み見等の情報の不正入手」（234件）、「インターネットショッピングでの不正購入」（172件）の順となっている。

図１－３　令和２年における不正アクセス後の行為別認知件数

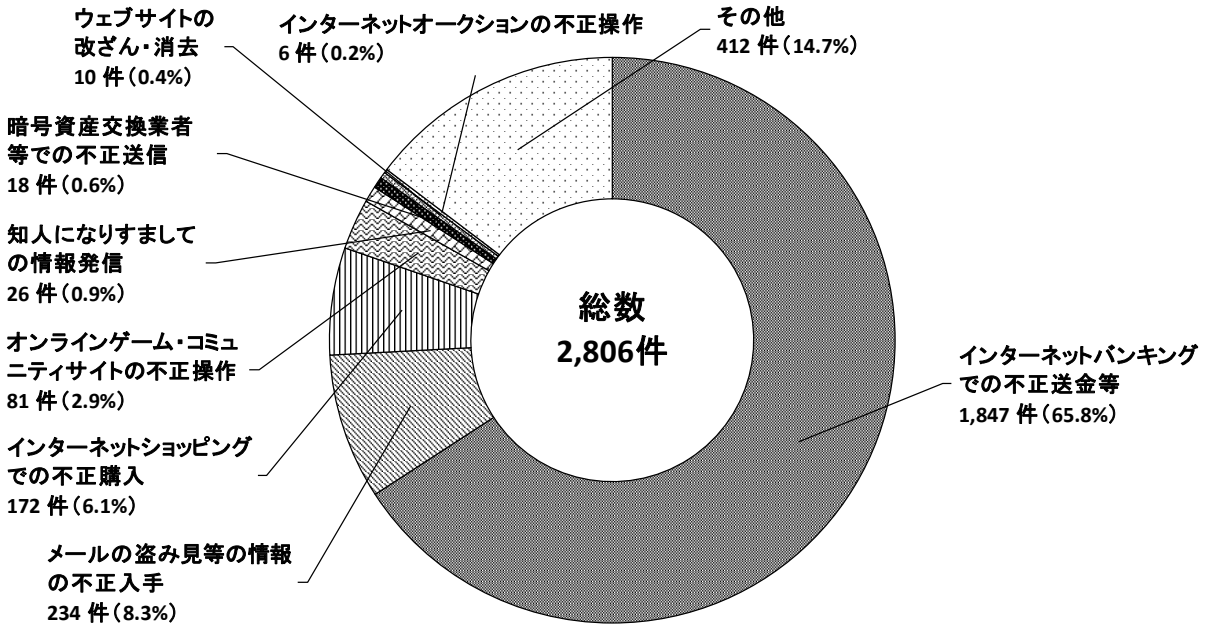


表１－３　不正アクセス後の行為別認知件数（過去５年）

区分＼年次	平成28年	平成29年	平成30年	令和元年	令和２年
インターネットバンキングでの不正送金等	1,305	442	330	1,808	1,847
メールの盗み見等の情報の不正入手	91	146	385	329	234
インターネットショッピングでの不正購入	172	133	149	376	172
オンラインゲーム・コミュニティサイトの不正操作	124	83	199	60	81
知人になりすましての情報発信	25	110	24	30	26
暗号資産交換業者等での不正送信		149	169	22	18
ウェブサイトの改ざん・消去	6	14	13	19	10
インターネットオークションの不正操作	34	28	29	47	6
その他	83	97	188	269	412
計	1,840	1,202	1,486	2,960	2,806

※　平成28年以前は、「暗号資産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２年における不正アクセス禁止法違反事件の検挙件数・検挙人員は609件・230人であり、前年（令和元年）と比べ、207件・４人減少した。

検挙件数・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585件・216人といずれも全体の90%以上を占めており、このほか、「識別符号取得行為[注5]」が３件・３人、「識別符号提供（助長）行為[注6]」が４件・４人、「識別符号保管行為[注7]」が14件・13人、「識別符号不正要求行為[注8]」が３件・５人であった。

表２－１　違反行為別検挙件数等（過去５年）

区分＼年次		平成28年	平成29年	平成30年	令和元年	令和２年
不正アクセス行為	検挙件数	462	599	520	787	585
	検挙事件数[注9]	175	216	160	218	199
	検挙人員	192	242	164	222	216
識別符号取得行為	検挙件数	6	5	22	5	3
	検挙事件数	3	3	1	4	3
	検挙人員	3	5	2	4	3
識別符号提供（助長）行為	検挙件数	5	9	4	9	4
	検挙事件数	2	6	4	6	4
	検挙人員	3	12	4	9	4
識別符号保管行為	検挙件数	28	31	16	13	14
	検挙事件数	6	2	9	5	13
	検挙人員	6	6	12	7	13
識別符号不正要求行為	検挙件数	1	4	2	2	3
	検挙事件数	1	3	2	1	2
	検挙人員	1	4	2	1	5
計	検挙件数	502	648	564	816	609
	検挙事件数	182 (重複5)	227 (重複3)	170 (重複6)	232 (重複2)	207 (重複 14)
	検挙人員	200 (重複5)	255 (重複14)	173 (重複11)	234 (重複9)	230 (重複11)

※　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している。

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、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　検挙事件数とは、事件単位ごとに計上した数であり、一連の捜査で複数の犯罪を検挙した場合は１事件として計上する。

(2)　不正アクセス行為の手口別検挙状況

令和２年における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[注10]」が576件と全体の90%以上を占めている。

表２－２　不正アクセス行為の手口別検挙件数等（過去５年）

区分＼年次		平成28年	平成29年	平成30年	令和元年	令和２年
識別符号窃用型	検挙件数	457	545	502	785	576
	検挙事件数	174	213	155	216	190
セキュリティ・ホール攻撃型	検挙件数	5	54	18	2	9
	検挙事件数	3	5	6	2	9
計	検挙件数	462	599	520	787	585
	検挙事件数	175 (重複2)	216 (重複2)	160 (重複1)	218	199

※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している。

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

令和２年に検挙した不正アクセス禁止法違反事件に係る被疑者の年齢は、「20～29歳」が最も多く（103人）、次いで「30～39歳」（52人）、「14～19歳」（48人）の順となっている[注11]。

なお、令和２年に不正アクセス禁止法違反で補導又は検挙された者のうち、最年少の者は11歳[注12]、最年長の者は62歳であった。

図３－１　令和２年に検挙した不正アクセス禁止法違反事件の年齢別被疑者数

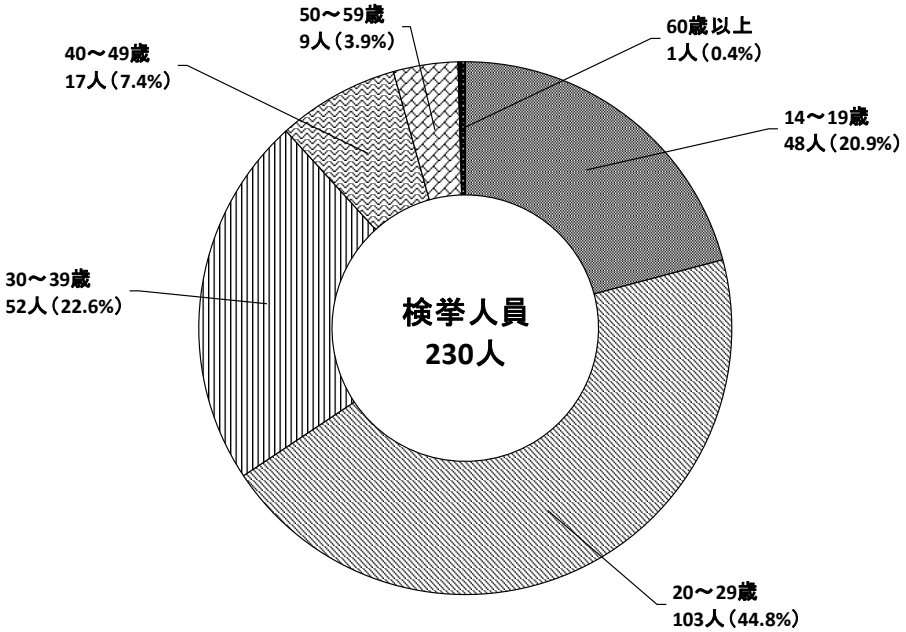


表３－１　年齢別被疑者数の推移（過去５年）

区分＼年次	平成28年	平成29年	平成30年	令和元年	令和２年
14～19歳	62	92	48	55	48
20～29歳	56	87	48	93	103
30～39歳	48	36	37	50	52
40～49歳	29	28	26	22	17
50～59歳	3	11	10	12	9
60歳以上	2	1	4	2	1
計	200	255	173	234	230

(2)　被疑者と利用権者の関係

令和２年に検挙した不正アクセス禁止法違反事件について、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、「交友関係のない他人によるもの」が最も多く（109人）、次いで「元交際相手や元従業員等の顔見知りの者によるもの」（108人）、「ネットワーク上の知り合いによるもの」（13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で、14歳未満の少年７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、検挙件数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別検挙件数

令和２年に検挙した不正アクセス禁止法違反の検挙件数について、識別符号窃用型の不正アクセス行為の手口別に内訳を見ると、「フィッシングサイトにより入手したもの」が最も多く（172件）、次いで「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」（115件）の順となっており、前年（令和元年）と比べ、前者は172倍、後者は約5.8倍となっている。

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

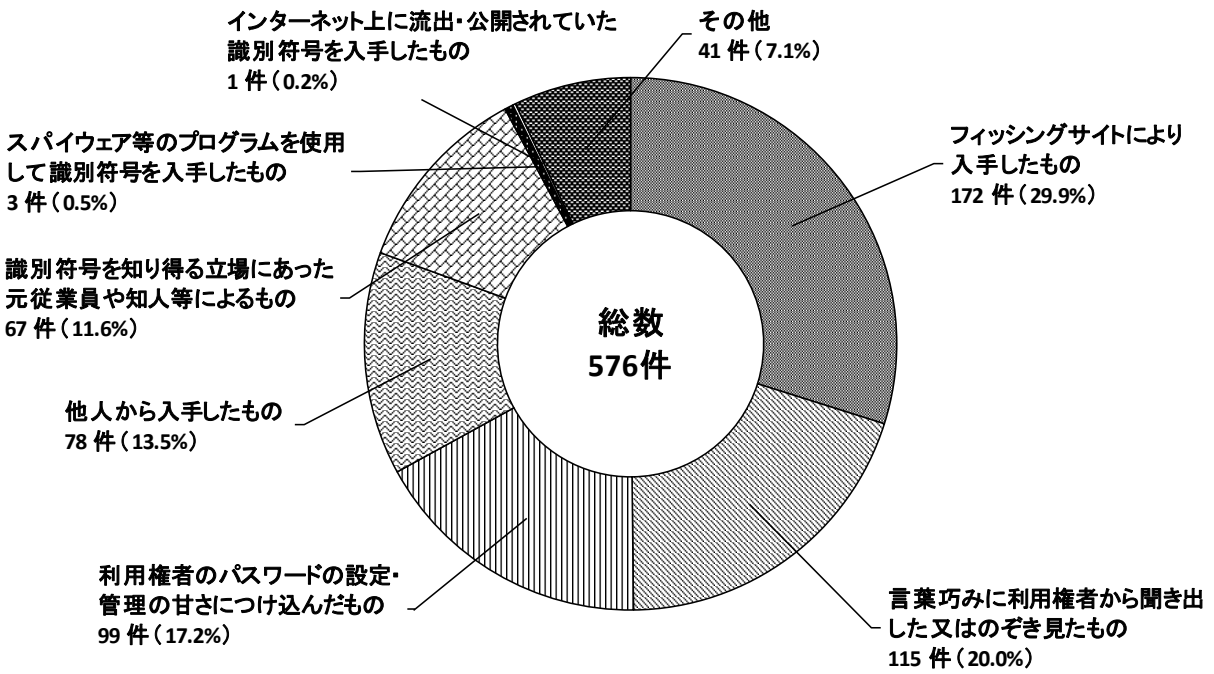


表３－２　不正アクセス行為の手口別検挙件数（過去５年）

区分＼年次	平成28年	平成29年	平成30年	令和元年	令和２年
識別符号窃用型	457	545	502	785	576
フィッシングサイトにより入手したもの	3	2	3	1	172
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	42	17	20	115
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	244	230	278	310	99
他人から入手したもの	20	74	13	182	78
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	113	131	161	67
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	34	37	0	5	3
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	4	0	7	3	1
その他	42	47	53	103	41
セキュリティ・ホール攻撃型	5	54	18	2	9

注13　コンピュータ内のファイル情報、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別検挙件数

令和２年に検挙した不正アクセス禁止法違反の検挙件数について、不正アクセス行為の動機別に内訳を見ると、「不正に経済的利益を得るため」が最も多く（274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」（138件）、「好奇心を満たすため」（78件）の順となっている。

図３－３　令和２年における不正アクセス行為の動機別検挙件数

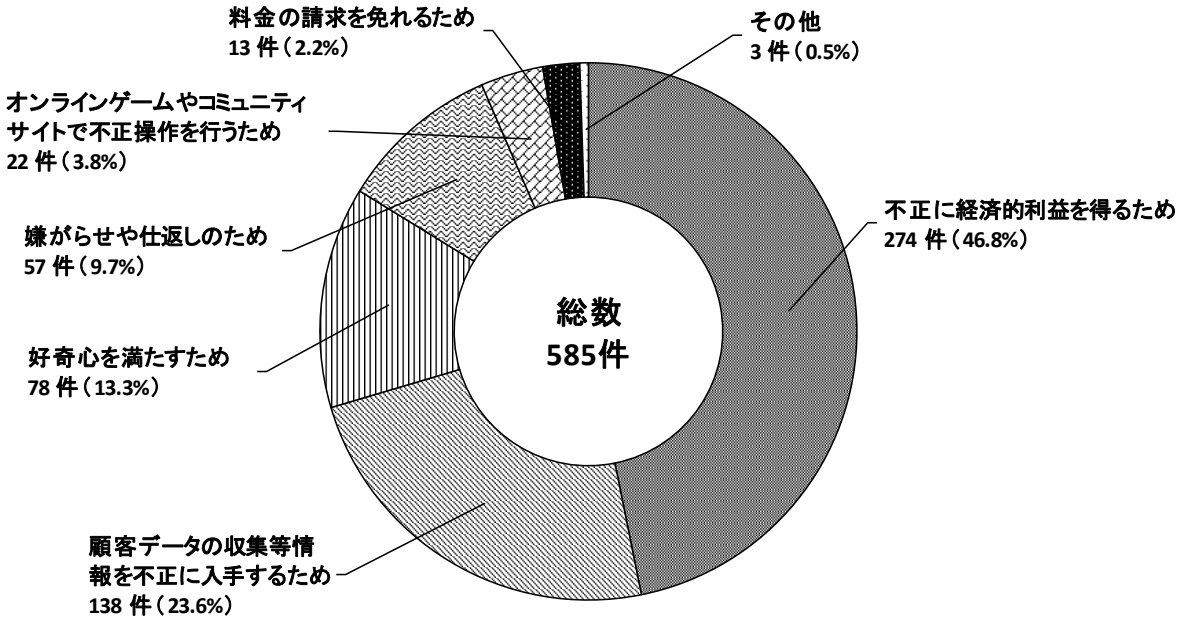


表３－３　不正アクセス行為の動機別検挙件数（過去５年）

区分＼年次	平成28年	平成29年	平成30年	令和元年	令和２年
不正に経済的利益を得るため	41	93	22	333	274
顧客データの収集等情報を不正に入手するため	70	103	195	254	138
好奇心を満たすため	208	193	103	52	78
嫌がらせや仕返しのため	44	59	46	68	57
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	43	43	101	17	22
料金の請求を免れるため	25	86	15	54	13
その他	31	22	38	9	3
計	462	599	520	787	585

(5)　不正に利用されたサービス別検挙件数

令和２年に検挙した不正アクセス禁止法違反の検挙件数のうち、識別符号窃用型の不正アクセス行為（576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見ると、「社員・会員用等の専用サイト」が最も多く（174件）、次いで「オンラインゲーム・コミュニティサイト」（88件）の順となっており、前年（令和元年）と比べ、前者は15.2%の増加、後者は約60.7%の減少となっている。

図３－４　令和２年における不正アクセス行為（識別符号窃用型）により不正に利用されたサービス別検挙件数

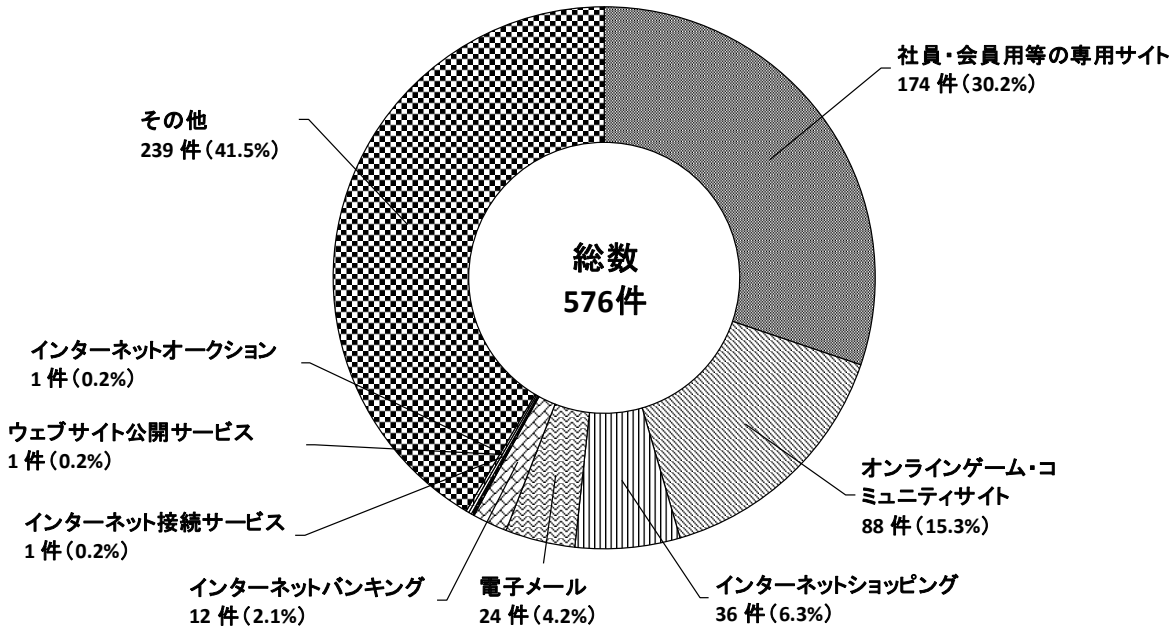


表３－４　不正アクセス行為（識別符号窃用型）により不正に利用されたサービス別検挙件数（過去５年）

区分＼年次	平成28年	平成29年	平成30年	令和元年	令和２年
社員・会員用等の専用サイト	40	116	200	151	174
オンラインゲーム・コミュニティサイト	185	210	217	224	88
インターネットショッピング	18	22	9	67	36
電子メール	136	92	34	21	24
インターネットバンキング	13	8	7	14	12
インターネット接続サービス	5	2	9	5	1
ウェブサイト公開サービス	2	7	3	5	1
インターネットオークション	9	11	6	4	1
その他	49	77	17	294	239
計	457	545	502	785	576

４　令和２年の主な検挙事例

(1)　アルバイトの男(32)は､平成31年１月から２月までの間､元勤務先の会社のＩＤ・パスワードを無断で使用してインターネット通販サイトに不正にアクセスした上、ギフト券を不正に注文し窃取した｡令和２年２月､男を不正アクセス禁止法違反(不正アクセス行為)、窃盗罪等で検挙した。(京都府)

(2)　アルバイトの男（25）は、平成29年12月から令和元年５月までの間、元交際相手のＩＤ・パスワードを無断で使用して同人のＳＮＳアカウントに不正にアクセスし､同アカウントを乗っ取り､同人を誹謗中傷する内容を投稿して名誉を毀損した。令和２年２月、男を不正アクセス禁止法違反（不正アクセス行為)、名誉毀損罪等で検挙した。(広島県)

(3)　会社員の男（21）は、令和２年１月、他人のＩＤ・パスワードを使用して電気通信事業者が提供するポイントサイトに不正にアクセスした上、他人のアカウントに保管されたポイントを使用して電子書籍等を購入した。同年８月、男を不正アクセス禁止法違反（不正アクセス行為）及び電子計算機使用詐欺罪で検挙した。（三重県）

(4)　無職の男（46）は、令和２年４月、元同僚のＩＤ・パスワードを使用して元勤務先のメールサーバに不正にアクセスし、同社内のメールを盗み見た上、同メールを取引先の企業に転送し漏えいさせた。同年７月、男を不正アクセス禁止法違反（不正アクセス行為）で検挙した。(栃木県)

(5)　会社員の男（33）は、令和元年12月、顧客から預かっていた携帯電話端末を操作し、同人のＩＤ・パスワードを無断で使用してインターネットショッピングサイトに不正にアクセスした上､ギフト券をキャリア決済により購入した｡令和２年８月、男を不正アクセス禁止法違反（不正アクセス行為）及び電子計算機使用詐欺罪で検挙した。(山形県)

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不正アクセス行為が発生していることから、ＩＤと同じパスワードや、利用権者の氏名、電話番号、生年月日等を用いた推測されやすいパスワードを設定しないほか、複数のウェブサイトで同じＩＤ・パスワードの組合せを使用しない（パスワードを使い回さない）よう注意する。また、日頃から自己のパスワードを適切に管理し、不用意にパスワードを他人に教えたり、インターネット上で入力・記録したりすることのないよう注意する。

(2)　フィッシングへの対策

金融機関や荷物の配送連絡を装ったＳＭＳ（ショートメッセージサービス）や電子メールを用いて、実在する企業を装ったフィッシングサイトへ誘導し、ＩＤ・パスワードを入力させる手口が多数確認されていることから、このようなＳＭＳや電子メールに記載されたリンク先のＵＲＬにアクセス等しないよう注意する。また、受信したＳＭＳや電子メールについては、送信元や本文に記載されたリンク先のＵＲＬをよく確認する。

(3)　不正プログラムへの対策

ＳＭＳからの誘導により携帯電話端末に不正なアプリをインストールさせ、当該アプリによって表示される偽の警告メッセージからフィッシングサイトへ誘導し、ＩＤ・パスワードを入力させる手口も確認されていることから、心当たりのある企業からのＳＭＳや電子メールであっても、当該企業から届いたＳＭＳや電子メールであることが確認できるまでは添付ファイルを開かず、本文に記載されたリンク先のＵＲＬをクリックしないよう徹底する。また、不特定多数が利用するコンピュータでは、ＩＤ・パスワード、クレジットカード情報等の重要な情報を入力しないよう徹底する。さらに、アプリ等のソフトウェアの不用意なインストールを避けるとともに、不正プログラムへの対策（ウイルス対策ソフト等の利用による不正プログラム対策のほか、オペレーティングシステムを含む各種ソフトウェアのアップデート等によるぜい弱性対策等）を適切に講ずる。特に、インターネットバンキング、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、不正プログラムへの対策が適切に講じられていることを確認するとともに、ワンタイムパスワード等の二要素認証[注14]や二経路認証[注15]を導入するなど、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)　運用体制の構築等

セキュリティの確保に必要なログの取得等の仕組みを導入するとともに、管理するシステムに係るぜい弱性の管理、不審なログインや行為等の監視及び不正にアクセスされた場合の対処に必要な体制を構築し、適切に運用する。

(2)　パスワードの適切な設定

前記のとおり、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

注14　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。

注15　インターネットバンキング等において、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、携帯電話端末等（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。

セス行為が発生していることから、使用する文字の数や種類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、複数のウェブサイトで同じＩＤ・パスワードの組合せを使用しない（パスワードを使い回さない）よう利用権者に周知するなどの措置を講ずる。

⑶　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、委託先業者等の者による不正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場合には、アクセス管理者が速やかに当該者に割り当てていたＩＤの削除又はパスワードの変更を行うなど、ＩＤ・パスワードの適切な管理を徹底する。

⑷　セキュリティ・ホール攻撃への対策

ウェブシステムやＶＰＮサーバのぜい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、定期的にサーバやアプリケーションのプログラムを点検し、セキュリティ上のぜい弱性を解消する。

⑸　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・パスワードを用いて不正にアクセスする手口や、フィッシング等により不正に取得された可能性のあるＩＤ・パスワードがインターネット上に流出する事案が確認されていることから、ワンタイムパスワード等の二要素認証や二経路認証の積極的な導入等により認証を強化する。また、自らが管理するシステムに係るフィッシング等の情報を日頃から収集し、フィッシングサイトが出回っていること、正規のウェブサイトであるかよく確認した上でアクセスする必要があること等について、利用権者に対して注意喚起を行う。

（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２年（令和２年１月１日から令和２年 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）の届出数は 187（令和元年：89）であった（注２）。令和２年は令和元年と比べて、98（約 110%）増加した。

届出の被害内容について、主に見受けられたものは、会員制サイトのログイン画面に対する、パスワードリスト型攻撃等の不正なログインを試行するものであった。

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つの届出につい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件数は届出数に必ずしも一致しない。

(1) 手口別分類

届出を攻撃行為（手口）により分類したものである。総計は 425 件（令和元年：126 件）であった（１つの届出について複数の攻撃行為を受けている場合があるため、届出数とは一致していない）。

ア　侵入行為

侵入行為に係る攻撃等に分類した件数は 280 件（令和元年：59 件）であった。

(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の行為である。

７件あり、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のいわゆるセキュリティホールを悪用した攻撃、システムの設定不備を悪用した攻撃等により権限を不正に取得して侵入する行為である。

100 件あり、その主な内容を次に示す。

【主な内容】

ソフトウェアのバグを悪用した攻撃：37 件

システムの設定不備を悪用した攻撃：32 件

パスワード推測：31 件

(ｳ) 不正行為の実行及び目的達成後の行為

侵入その他、何らかの原因による不正行為の実行である。

173 件あり、その主な内容を次に示す。

【主な内容】

ファイル／データ窃取、改ざん等：125 件

不正プログラムの埋込：28 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、２件（令和元年：12 件）であった。

ウ その他

その他にはメール不正中継や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、143 件（令和元年：55 件）あり、その主な内容を次に示す。

【主な内容】

正規ユーザへのなりすまし：73 件

メール不正中継：４件

ソーシャルエンジニアリング：３件

(2) 原因別分類

187 の届出のうち、実際に被害に遭った 143 の届出について、不正アクセスの原因となった問題点／弱点で分類したものである。総計は 156 件（令和元年：56 件）であった（１つの届出について複数の被害原因が存在する場合があるため、届出数とは一致していない）。

被害原因として最も多いものは「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）」であった。これはウェブシステムの管理画面へのアクセス制限の不備や、システム開発環境等で使用者を限定しているはずの環境であるがゆえにセキュリティ設定が不十分となってしまった等、セキュリティ上問題のあるサーバのセキュリティ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、「原因不明」の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。

主な被害原因を次に示す。

【主な被害原因】

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：32 件
古いバージョンの利用や、修正プログラム・必要なプラグイン等の未導入によるもの：27 件
ログイン試行（パスワードリスト型攻撃等）：17 件
原因不明：27 件

(3) 電算機分類

届出を不正アクセス行為の対象となった機器で分類したものである。
１つの届出において、複数の機器に不正アクセスを受けている場合がある。
【主な機器】
ウェブサーバ：63 件
クライアント：31 件
データベースサーバ：23 件

(4) 被害内容分類

届出のうち、実際に被害に遭った届出を被害内容で分類したものである。総計 256 件（令和元年：82 件）であった（１つの届出に複数の被害内容が存在する場合があるため、届出数とは一致していない）。

なお、対処に係る作業発生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。

主な内容を次に示す。

【主な被害内容】
データの窃取や盗み見：104 件
オンラインサービスの不正利用：39 件
ファイルの書き換え：39 件

(5) 対策情報

冒頭で述べた通り、令和２年は会員制サイトへのパスワードリスト攻撃等のログイン試行による不正ログインが原因の、会員情報窃取やポイント交換の被害が多く見られた。また、EC サイトの改ざん等によるクレジットカード情報の窃取や、システムのデータベースを消去または暗号化してデータの復旧のために身代金を要求するような脅迫文を残すといった被害も依然として見られた。

これらを含む、原因別で分類した 156 件の原因を割合で示すと「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 32 件（約 20.5%）、「古いバージョンの利用や、修正プログラム・必要なプラグイン等の未導入によるもの」が 27 件（約 17.3%）であり、この２つの項目で 59 件（約 37.8%）と大きな割合を占めている。また、ログイン試行（パスワードリスト型攻撃等）が

17 件（約 10.9%）を占める。
　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、次のような対策を検討していただきたい。

システム管理者向け対策としては、
- サーバのアクセス権の適切な設定
- ウェブアプリケーションの定期的な脆弱性対策の実施
- サーバ上の不要なサービスの停止
- ウェブサイトへの大量ログイン試行によるアクセス発生の警告表示や遮断機能の導入

等、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や不正ログインを早急に検知できる機能の追加を検討することが推奨される。

また、ユーザ向け対策としては、
- 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
- 二要素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

等、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カ、バージョンチェッカ）

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　ここに挙げた数は、コンピュータ不正アクセスの届出を IPA が受理した数であり、不正アクセスやサイバー攻撃等に関して実際の発生数や被害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２年（令和２年１月１日から令和２年 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 43,823 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 28,447 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 4,161 件の報告があった。

[1/1-3/31: 713 件、4/1-6/30: 982 件、7/1-9/30: 1,380 件、10/1-12/31: 1,086 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 1,261 件の報告があった。

[1/1-3/31: 192 件、4/1-6/30: 291 件、7/1-9/30: 374 件、10/1-12/31: 404 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 742 件の報告があった。

[1/1-3/31: 250 件、4/1-6/30: 133 件、7/1-9/30: 158 件、10/1-12/31: 324 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 94 件の報告があった。

[1/1-3/31: 21 件、4/1-6/30: 70 件、7/1-9/30: 8 件、10/1-12/31: 5 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 19,961 件の報告があった。
[1/1-3/31: 3,839 件、4/1-6/30: 5,262 件、7/1-9/30: 5,845 件、10/1-12/31: 5,015 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、マルウエア感染や情報の窃取などを試みる攻撃について 34 件の報告があった。
[1/1-3/31: 2 件、4/1-6/30: 6 件、7/1-9/30: 16 件、10/1-12/31: 10 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 2,061 件の報告があった。
[1/1-3/31: 492 件、4/1-6/30: 379 件、7/1-9/30: 605 件、10/1-12/31: 585 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]

2020 年 1 月	2020 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 2020 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注意喚起 複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起 Microsoft Internet Explorer の未修正の脆弱性 (CVE-2020-0674) に関する注意喚起 Firefox の脆弱性 (CVE-2019-17026) に関する注意喚起

2020 年 2 月	2020 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 Adobe Flash Player の脆弱性（APSB20-06）に関する注意喚起 Adobe Acrobat および Reader の脆弱性（APSB20-05）に関する注意喚起 Apache Tomcat の脆弱性（CVE-2020-1938）に関する注意喚起
2020 年 3 月	2020 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 Microsoft SMBv3 の脆弱性（CVE-2020-0796）に関する注意喚起 ウイルスバスター ビジネスセキュリティの脆弱性（CVE-2020-8468）に関する注意喚起 Apex One およびウイルスバスター コーポレートエディションの脆弱性（CVE-2020-8467、CVE-2020-8468）に関する注意喚起 Adobe Acrobat および Reader の脆弱性（APSB20-13）に関する注意喚起 Adobe Type Manager ライブラリ の未修正の脆弱性に関する注意喚起
2020 年 4 月	2020 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 2020 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 OpenSSL の脆弱性（CVE-2020-1967）に関する注意喚起
2020 年 5 月	Oracle WebLogic Server の脆弱性に関する注意喚起 SaltStack Salt の複数の脆弱性（CVE-2020-11651, CVE-2020-11652）に関する注意喚起 2020 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 Acrobat および Reader の脆弱性（APSB20-24）に関する注意喚起 Apache Tomcat の脆弱性（CVE-2020-9484）に関する注意喚起 ISC BIND 9 の脆弱性（CVE-2020-8616, CVE-2020-8617）に関する注意喚起
2020 年 6 月	2020 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（APSB20-30）に関する注意喚起
2020 年 7 月	Microsoft Windows Codecs Library の脆弱性（CVE-2020-1425, CVE-2020-1457）に関する注意喚起 複数の BIG-IP 製品の脆弱性（CVE-2020-5902）に関する注意喚起 2020 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 2020 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
2020 年 8 月	SKYSEA Client View の脆弱性（CVE-2020-5617）に関する注意喚起 2020 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（APSB20-48）に関する注意喚起

	Apache Struts 2 の脆弱性（S2-059、S2-060）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
2020 年 9 月	2020 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 複数の MobileIron 製品の脆弱性に関する注意喚起
2020 年 10 月	Adobe Flash Player の脆弱性（APSB20-58）に関する注意喚起 2020 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 2020 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
2020 年 11 月	Adobe Acrobat および Reader の脆弱性（APSB20-67）に関する注意喚起 2020 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 Cisco Security Manager の複数の脆弱性に関する注意喚起
2020 年 12 月	ファイル・データ転送アプライアンス FileZen に関する注意喚起 Apache Tomcat の脆弱性（CVE-2020-17527）に関する注意喚起 OpenSSL の脆弱性（CVE-2020-1971）に関する注意喚起 2020 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 Apache Struts 2 の脆弱性（S2-061）に関する注意喚起 Adobe Acrobat および Reader の脆弱性（APSB20-75）に関する注意喚起

（２） 活動概要（報告状況等の公表）

発行日：2020/1/21［2019 年 10 月 1 日～2019 年 12 月 31 日］
発行日：2020/1/21［2019 年 10 月 1 日～2019 年 12 月 31 日］
発行日：2020/7/14［2020 年 4 月 1 日～2020 年 6 月 30 日］
発行日：2020/10/15［2020 年 7 月 1 日～2020 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］363 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。