令和４年４月７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、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。

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

令和３年１月１日から同年12月31日までの間における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に関する技術の研究開発の状況及び募集・調査した民間企業等における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。

３　掲載先（ウェブサイト）

○　国家公安委員会　https://www.npsc.go.jp/
○　総　務　省　https://www.soumu.go.jp/
○　経済産業省　https://www.meti.go.jp/

不正アクセス行為の発生状況

第１　令和３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

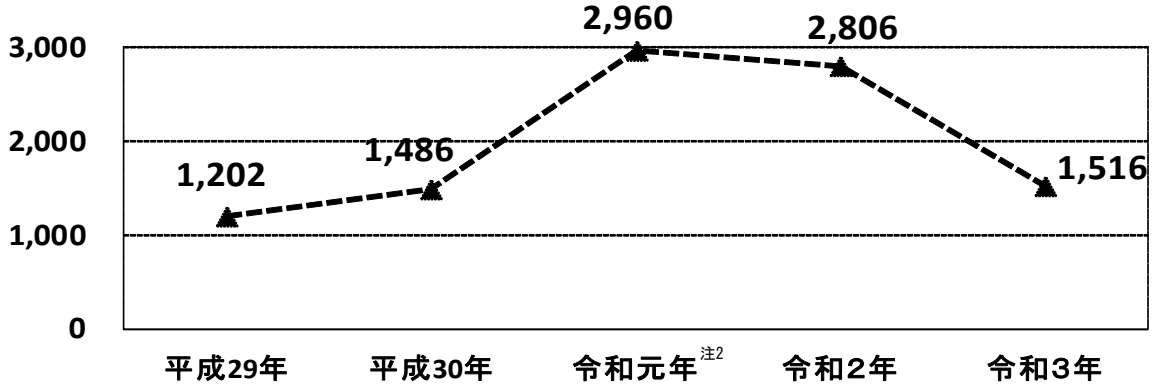
令和３年に都道府県警察から警察庁に報告がなされた不正アクセス行為の認知・検挙状況等は次のとおりである。

１　不正アクセス行為の認知状況

(1)　認知件数

令和３年における不正アクセス行為の認知件数[注1]は1,516件であり、前年（令和２年）と比べ、1,290件（約46.0%）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３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（1,492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29年	平成30年	令和元年	令和2年	令和3年
一般企業	1,177	1,314	2,855	2,703	1,492
行政機関等	9	6	90	84	15
プロバイダ	6	4	6	5	5
大学、研究機関等	5	161	3	11	4
その他	5	1	6	3	0
計	1,202	1,486	2,960	2,806	1,516

※「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３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、「利用権者[注4]からの届出」が最も多く（716件）、次いで「警察活動」（578件）、「アクセス管理者からの届出からの届出」（209件）の順となっている。

図１－２　令和３年における端緒別認知件数

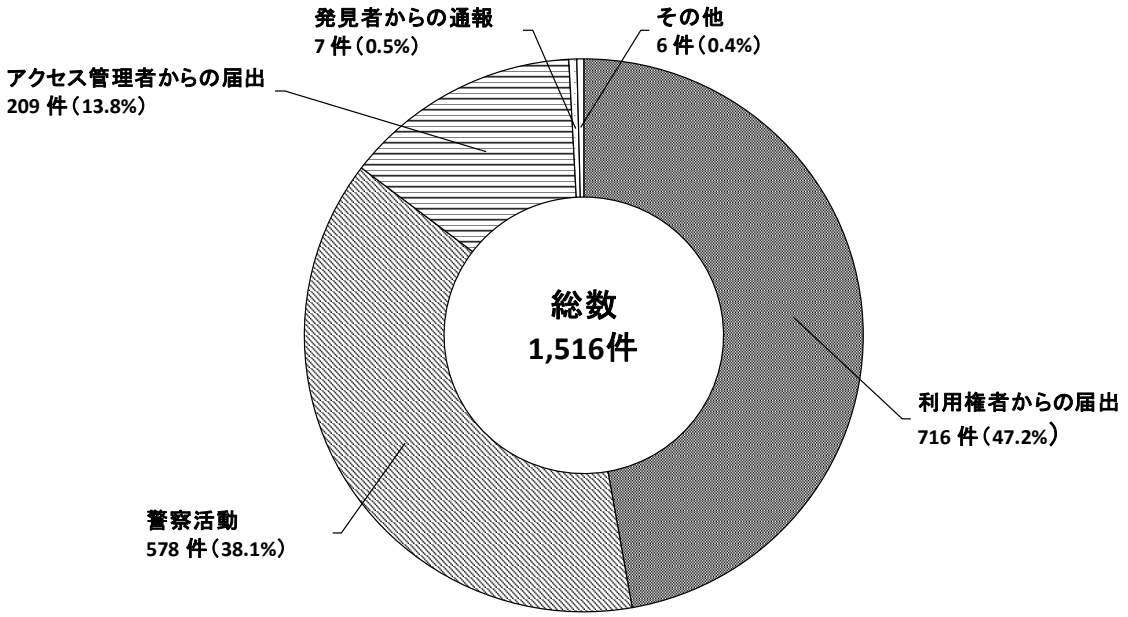


表１－２　端緒別認知件数（過去５年）

区分＼年次	平成29年	平成30年	令和元年	令和2年	令和3年
利用権者からの届出	655	852	761	567	716
警察活動	283	269	1,555	1,608	578
アクセス管理者からの届出	255	345	602	614	209
発見者からの通報	6	16	9	5	7
その他	3	4	33	12	6
計	1,202	1,486	2,960	2,806	1,516

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３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（693件）、次いで「インターネットショッピングでの不正購入」（349件）、「メールの盗み見等の情報の不正入手」（175件）の順となっている。

図１－３　令和３年における不正アクセス後の行為別認知件数

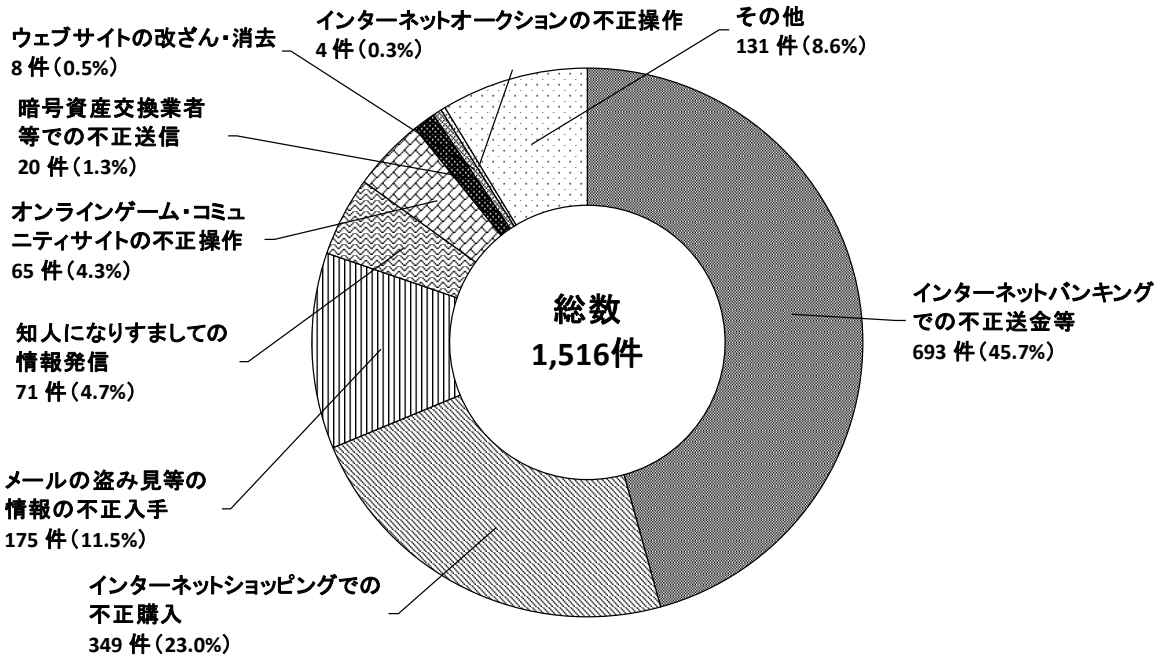


表１－３　不正アクセス後の行為別認知件数（過去５年）

区分＼年次	平成29年	平成30年	令和元年	令和2年	令和3年
インターネットバンキングでの不正送金等	442	330	1,808	1,847	693
インターネットショッピングでの不正購入	133	149	376	172	349
メールの盗み見等の情報の不正入手	146	385	329	234	175
知人になりすましての情報発信	110	24	30	26	71
オンラインゲーム・コミュニティサイトの不正操作	83	199	60	81	65
暗号資産交換業者等での不正送信	149	169	22	18	20
ウェブサイトの改ざん・消去	14	13	19	10	8
インターネットオークションの不正操作	28	29	47	6	4
その他	97	188	269	412	131
計	1,202	1,486	2,960	2,806	1,516

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３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429件・235人であり、前年（令和２年）と比べ、180件減少し、５人増加した。

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408件・227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４件・２人、「識別符号提供（助長）行為[注6]」が９件・８人、「識別符号保管行為[注7]」が７件・６人、「識別符号不正要求行為[注8]」が１件・１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29年	平成30年	令和元年	令和2年	令和3年
不正アクセス行為	検挙件数	599	520	787	585	408
	検挙事件数[注9]	216	160	218	199	189
	検挙人員	242	164	222	216	227
識別符号取得行為	検挙件数	5	22	5	3	4
	検挙事件数	3	1	4	3	2
	検挙人員	5	2	4	3	2
識別符号提供(助長)行為	検挙件数	9	4	9	4	9
	検挙事件数	6	4	6	4	8
	検挙人員	12	4	9	4	8
識別符号保管行為	検挙件数	31	16	13	14	7
	検挙事件数	2	9	5	13	6
	検挙人員	6	12	7	13	6
識別符号不正要求行為	検挙件数	4	2	2	3	1
	検挙事件数	3	2	1	2	1
	検挙人員	4	2	1	5	1
計	検挙件数	648	564	816	609	429
	検挙事件数	227 (重複3)	170 (重複6)	232 (重複2)	207 (重複14)	195 (重複11)
	検挙人員	255 (重複14)	173 (重複11)	234 (重複9)	230 (重複11)	235 (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すなどして、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３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398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29年	平成30年	令和元年	令和2年	令和3年
識別符号窃用型	検挙件数	545	502	785	576	398
	検挙事件数	213	155	216	190	182
セキュリティ・ホール攻撃型	検挙件数	54	18	2	9	10
	検挙事件数	5	6	2	9	8
計	検挙件数	599	520	787	585	408
	検挙事件数	216 （重複2）	160 （重複1）	218	199	189 （重複1）

※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特定電子計算機にネットワークを通じて他人の識別符号を入力して、当該特定電子計算機を作動させ、不正に利用できる状態にする行為をいう。

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３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（87人）、次いで「14～19歳」（60人）、「30～39歳」（43人）の順となっている[注11]。

なお、令和３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12歳[注12]、最年長の者は69歳であった。

図３－１　令和３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

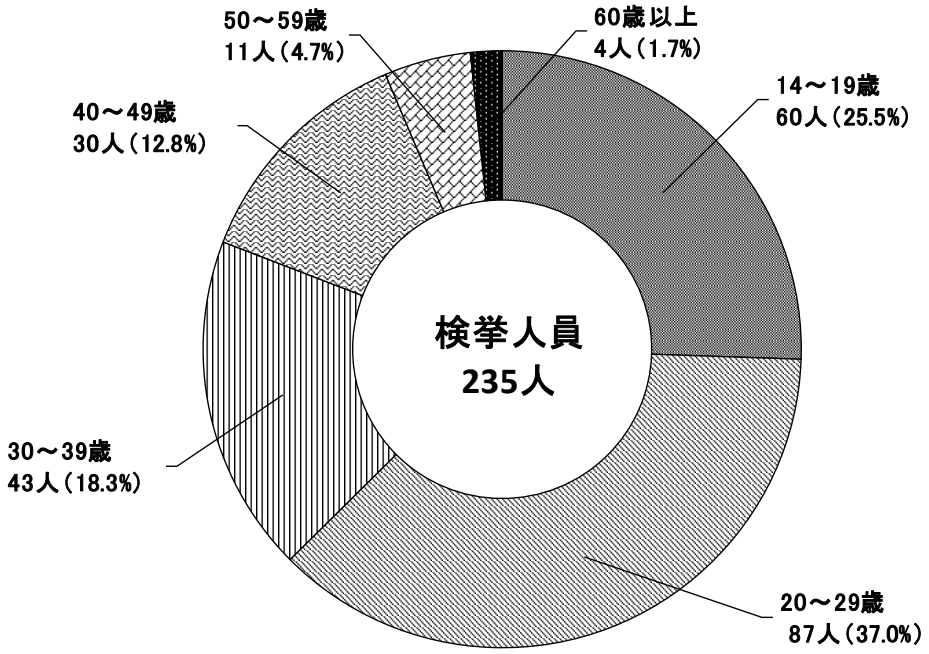


表３－１　年齢別被疑者数の推移（過去５年）

区分＼年次	平成29年	平成30年	令和元年	令和2年	令和3年
14～19歳	92	48	55	48	60
20～29歳	87	48	93	103	87
30～39歳	36	37	50	52	43
40～49歳	28	26	22	17	30
50～59歳	11	10	12	9	11
60歳以上	1	4	2	1	4
計	255	173	234	230	235

(2)　被疑者と利用権者の関係

令和３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、「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（129人）、次いで「交友関係のない他人によるもの」（95人）、「ネットワーク上の知り合いによるもの」（11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３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３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、「利用権者のパスワードの設定・管理の甘さにつけ込んで入手」が最も多く（153件）、次いで「フィッシングサイトにより入手」（70件）の順となっており、前年（令和２年）と比べ、前者は約1.55倍、後者は約0.41倍となっている。

図３－２　令和３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

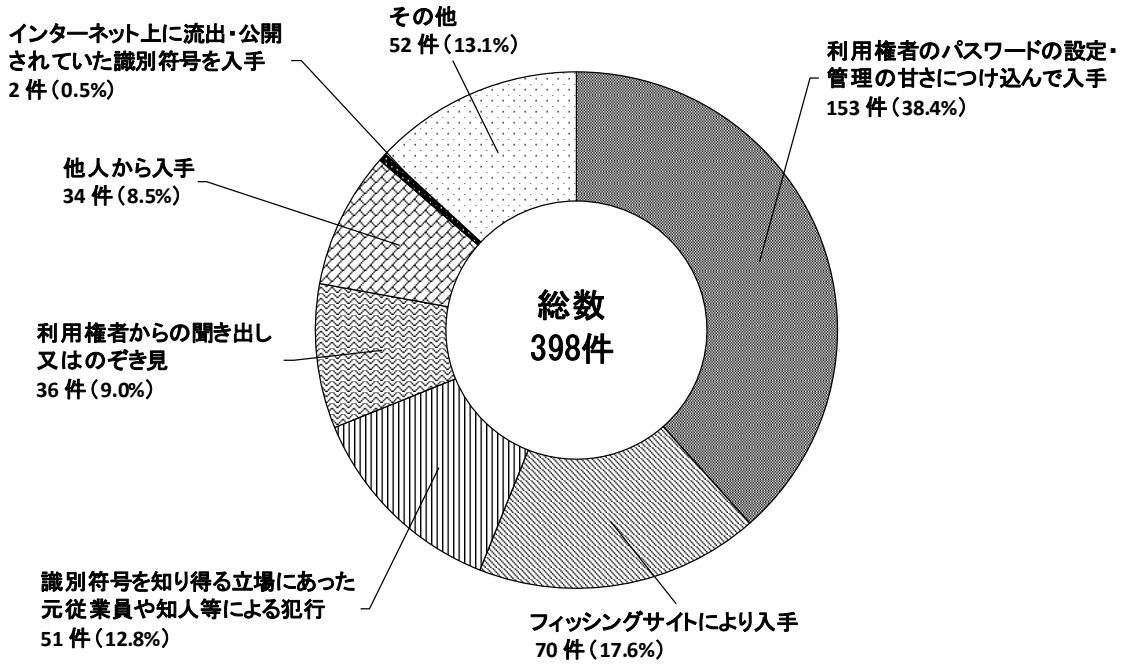


表３－２　不正アクセス行為の手口別検挙件数（過去５年）

区分＼年次	平成29年	平成30年	令和元年	令和2年	令和3年
識別符号窃用型	545	502	785	576	398
利用権者のパスワードの設定・管理の甘さにつけ込んで入手	230	278	310	99	153
フィッシングサイトにより入手	2	3	1	172	70
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犯行	113	131	161	67	51
利用権者からの聞き出し又はのぞき見	42	17	20	115	36
他人から入手	74	13	182	78	34
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	0	7	3	1	2
スパイウェア[注13]等のプログラムを使用して入手	37	0	5	3	0
その他	47	53	103	41	52
セキュリティ・ホール攻撃型	54	18	2	9	10

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３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（151件）、次いで「好奇心を満たすため」（130件）、「嫌がらせや仕返しのため」（59件）の順となっている。

図３－３　令和３年における不正アクセス行為の動機別検挙件数

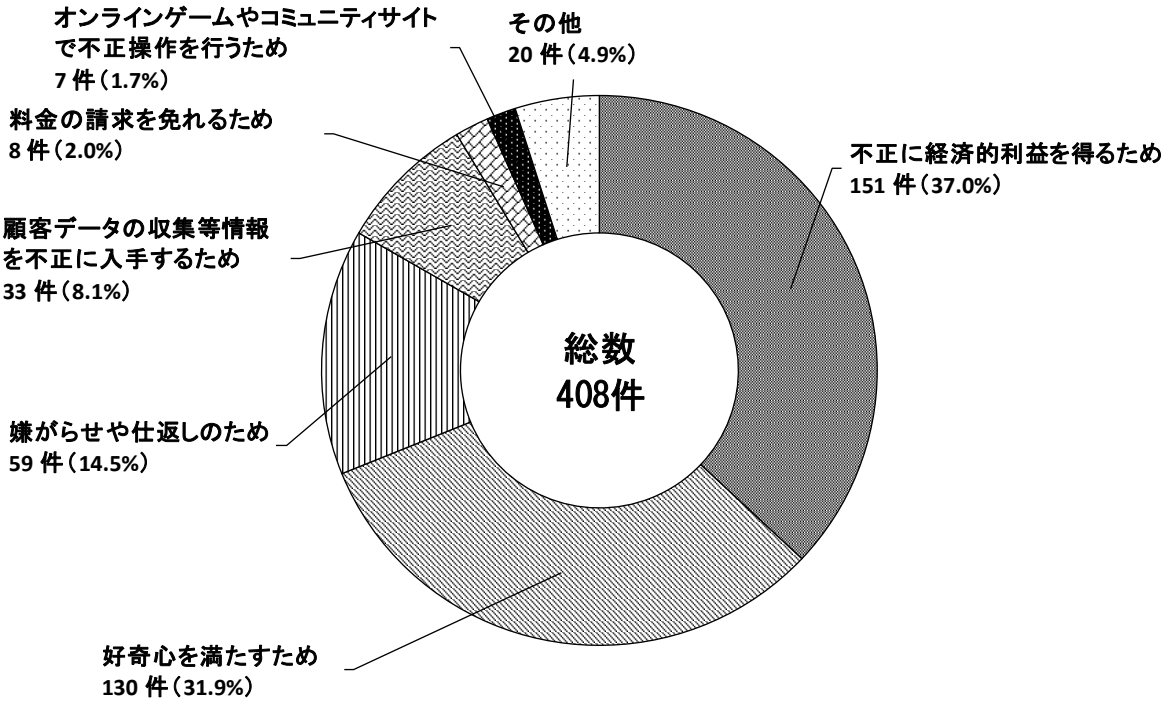


表３－３　不正アクセス行為の動機別検挙件数（過去５年）

区分＼年次	平成29年	平成30年	令和元年	令和2年	令和3年
不正に経済的利益を得るため	93	22	333	274	151
好奇心を満たすため	193	103	52	78	130
嫌がらせや仕返しのため	59	46	68	57	59
顧客データの収集等情報を不正に入手するため	103	195	254	138	33
料金の請求を免れるため	86	15	54	13	8
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	101	17	22	7
その他	22	38	9	3	20
計	599	520	787	585	408

(5)　不正に利用されたサービス別検挙件数

令和３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（398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、「オンラインゲーム・コミュニティサイト」が最も多く（144件）、次いで「インターネットバンキング」（96件）の順となっており、前年（令和２年）と比べ、前者は約1.64倍、後者は８倍となっている。

図３－４　令和３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

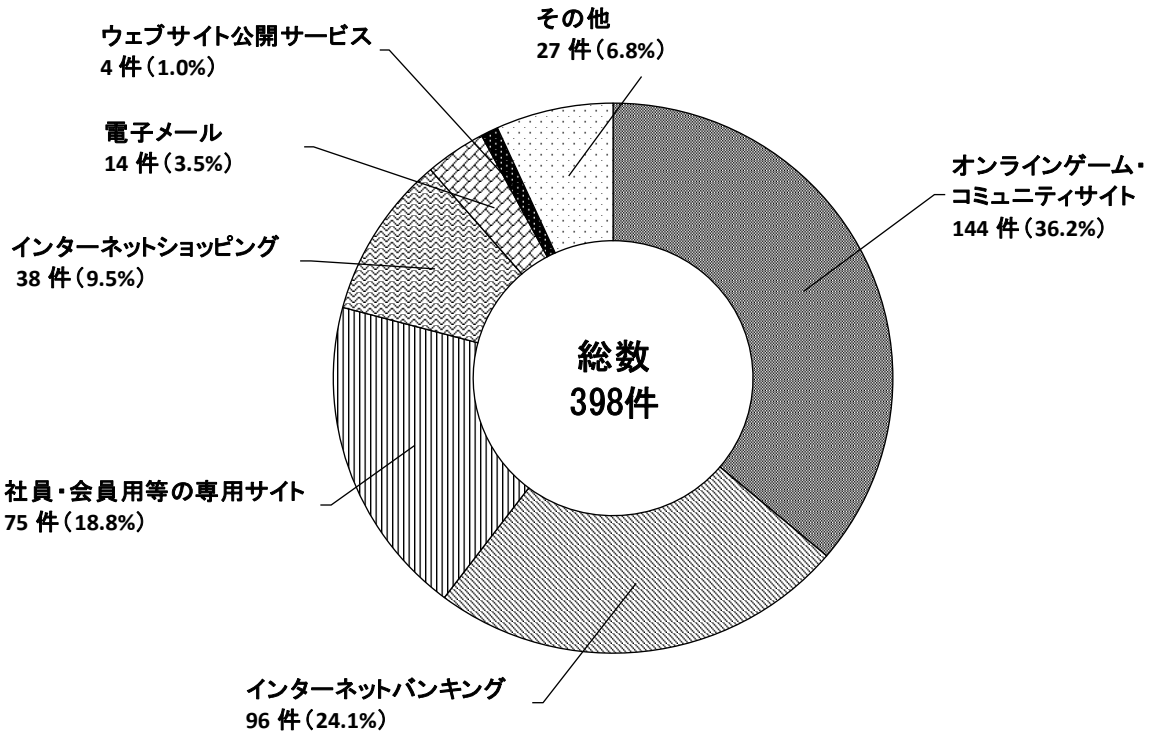


表３－４　不正アクセス行為（識別符号窃用型）により不正に利用されたサービス別検挙件数（過去５年）

区分＼年次	平成29年	平成30年	令和元年	令和2年	令和3年
オンラインゲーム・コミュニティサイト	210	217	224	88	144
インターネットバンキング	8	7	14	12	96
社員・会員用等の専用サイト	116	200	151	174	75
インターネットショッピング	22	9	67	36	38
電子メール	92	34	21	24	14
ウェブサイト公開サービス	7	3	5	1	4
インターネット接続サービス	2	9	5	1	0
インターネットオークション	11	6	4	1	0
その他	77	17	294	239	27
計	545	502	785	576	398

４　令和３年の主な検挙事例

⑴　会社員の女（21）は、令和２年４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スマートフォン決済サービスの認証サーバに不正アクセスし、インターネット通販サイトにおいてスニーカー等を注文して窃取した。令和３年１月、女を不正アクセス禁止法違反（不正アクセス行為）並びに私電磁的記録不正作出罪・同供用罪及び窃盗罪で検挙した。

⑵　無職の男（23）は、令和３年１月、元交際相手のＩＤ・パスワードを使用して元交際相手が利用するＳＮＳアカウントに不正アクセスし、元交際相手になりすまして投稿等を行った。同年３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。

⑶　会社員の男（42）は、平成31年２月、不正アクセス行為をする目的で、業務上知り得た顧客の証券口座のＩＤ・パスワードを自己の端末に不正に保管し、同証券口座から銀行口座に不正に送金するなどした。令和３年３月、男を不正アクセス禁止法違反（識別符号保管）、電子計算機使用詐欺罪等で検挙した。

⑷　学習支援業の男（37）は、令和２年９月、他人のＩＤ・パスワードを使用してインターネット通販サイトに不正アクセスし、パスワード及び登録電話番号を変更した上、電子マネーを不正に振替（チャージ）した。令和３年５月、男を不正アクセス禁止法違反（不正アクセス行為）並びに私電磁的記録不正作出罪・同供用罪及び電子計算機使用詐欺罪で検挙した。

⑸　会社員の男（37）は、令和２年11月、知人女性の個人情報を収集する目的で、同女のＩＤ・パスワードを使用してメールアカウントに不正アクセスし、登録情報やメール内容を閲覧した。令和３年６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。

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、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やアプリ等で同じ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。

なお、インターネット上に情報を保存するメモアプリ等が不正アクセスされ、保存していたパスワード等の情報が窃取されたと思われるケースも確認されていることから、情報の保存場所についても十分注意する。

(2)　フィッシングへの対策

eコマース関係企業、通信事業者、金融機関、荷物の配送連絡等を装った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、ＳＭＳや電子メールに記載されたリンク先のＵＲＬに不用意にアクセスしないよう注意する。

(3)　不正プログラムへの対策

通信事業者を装った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、当該アプリを実行すると表示されるログイン画面に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。

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。

(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､使用しなければならない文字数や種類を可能な限り増やすなど、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やアプリ等で同じ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。

(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、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速やかに行うなど、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。

(5)　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アクセスする手口が多数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、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３年（令和３年１月１日から令和３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）の届出件数は 243 件（令和２年：187 件）であった（注２）。令和３年は令和２年と比べて、56 件（約 29.9%）増加した。

届出の被害内容で主に見受けられたものは、VPN 装置の脆弱性を悪用した不正侵入、ウェブサイト（EC サイトを含む）の脆弱性を悪用した SQL インジェクション攻撃による情報窃取、そして業務委託先へのサイバー攻撃による情報窃取といったものであった。

次に、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件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 630 件（令和２年：425 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、届出件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 457 件（令和２年：280 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。

５件あり、ポートスキャンや脆弱性診断ツールを悪用したもの、アカウントの有効性確認を行うものなどであった。

(ｲ)　権限取得行為（侵入行為）

パスワード推測、システムの設定不備の悪用、またはソフトウェアのバグ等のいわゆる脆弱性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。

145 件あり、その主な内容を次に示す。

【主な内容】

脆弱性を悪用した攻撃：62 件

パスワード推測（パスワードリスト攻撃等）：45 件

システムの設定不備を悪用した攻撃：38 件

(ｳ) 不正行為の実行及び目的達成後の行為

侵入あるいは何らか別の方法によって行われた不正行為の内容である。307 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：198 件

資源利用(CPU 等のリソース不正使用)：56 件

不正プログラムの埋込：53 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して、サービスを利用不可又は低下させたりする攻撃で、２件（令和２年：２件）であった。

ウ その他

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である。171 件（令和２年：143 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：105 件

ソーシャルエンジニアリング：11 件

メール不正中継：１件

(2) 原因別分類

243 件の届出のうち、実際に被害に遭った 197 件の届出について、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 220 件（令和２年：156 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、届出件数とは一致していない)。

被害原因として最も多いものは、「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」であった。このうち、VPN 装置の脆弱性を悪用された例が多かった。これはコロナ禍のもと、テレワーク環境を整備する必要に迫られた企業・組織が、VPN 環境を構築するために、VPN 装置を急遽導入したり、ネットワーク機器の VPN 機能を有効にしたりといった対応により、環境構築を優先してセキュリティ対策が後回しとなるなど、対策不十分な状態で運用を続けた結果、その隙に乗じた攻撃の被害を受けたものと推測される。

また、「原因不明」のケースも依然として少なくはなく、調査が難しい手口

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】
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：51 件
原因不明：41 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）：39 件
ID、パスワード管理の不備：34 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：92 件
クラウドサーバ：86 件
クライアント：41 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。総計は 367 件（令和２年：256 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、届出件数とは一致していない）。
なお、対処に係る作業発生、サービスの一時停止、代替機の準備等の二次被害については除外している。
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：151 件
ファイルの書き換え：84 件
踏み台として悪用：51 件

(5) 対策情報
冒頭で述べた通り、令和３年は VPN 装置の脆弱性を悪用した不正侵入の被害が多く見られた。また、EC サイトの脆弱性を悪用した改ざん等による、クレジットカード情報の窃取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 220 件の原因を割合で示すと「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」が約 23.2%（51 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)」が約 17.7%（39 件）であり、この２つの項目で約 40.9%（90 件）と大きな割合を占めている。また、「ID、パスワード管理の不備」が約 15.5%（34 件）を占める。

VPN 装置や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、

- ネットワーク機器を含め、使用している機器やソフトウェアに関する、脆弱性情報の収集や修正プログラムの適用
- ウェブアプリケーションの定期的な脆弱性対策の実施
- サーバやネットワーク機器のアクセス権の適切な設定
- 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発生の警告表示や遮断機能の導入

等、脆弱性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
- 多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」
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/

コンピュータ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３年（令和３年１月１日から令和３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 44,242 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 32,677 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 4,772 件の報告があった。

[1/1-3/31: 1,085 件、4/1-6/30: 1,385 件、7/1-9/30: 1,291 件、10/1-12/31: 1,011 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 2,018 件の報告があった。

[1/1-3/31: 282 件、4/1-6/30: 251 件、7/1-9/30: 579 件、10/1-12/31: 906 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 701 件の報告があった。

[1/1-3/31: 138 件、4/1-6/30: 38 件、7/1-9/30: 119 件、10/1-12/31: 406 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 33 件の報告があった。

[1/1-3/31: 2 件、4/1-6/30: 8 件、7/1-9/30: 7 件、10/1-12/31: 16 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 23,108 件の報告があった。
[1/1-3/31: 4,831 件、4/1-6/30: 4,841 件、7/1-9/30: 6,311 件、10/1-12/31: 7,125 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 17 件の報告があった。
[1/1-3/31: 7 件、4/1-6/30: 5 件、7/1-9/30: 4 件、10/1-12/31: 1 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 2,028 件の報告があった。
[1/1-3/31: 763 件、4/1-6/30: 449 件、7/1-9/30: 474 件、10/1-12/31: 342 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]

2021 年 1 月	2021 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 (公開) Apache Tomcat の脆弱性 (CVE-2021-24122) に関する注意喚起 (公開) 2021 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 (公開) Pepperl+Fuchs 社の IO-Link Master シリーズの複数の脆弱性に関する注意喚起 (公開) sudo の脆弱性 (CVE-2021-3156) に関する注意喚起 (公開) sudo の脆弱性 (CVE-2021-3156) に関する注意喚起 (更新)
2021 年 2 月	SonicWall 製 SMA100 シリーズの脆弱性 (CVE-2021-20016) に関する注意喚起 (公開) SonicWall 製 SMA100 シリーズの脆弱性 (CVE-2021-20016) に関する注意喚起 (更新)

	2021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（公開） Adobe AcrobatおよびReaderの脆弱性（APSB21-09）に関する注意喚起（公開） FileZenの脆弱性（CVE-2021-20655）に関する注意喚起（公開） ISC BIND 9の脆弱性（CVE-2020-8625）に関する注意喚起（公開） SonicWall製SMA100シリーズの脆弱性（CVE-2021-20016）に関する注意喚起（更新） VMware vCenter Serverの脆弱性（CVE-2021-21972）に関する注意喚起（公開）
2021年3月	VMware vCenter Serverの脆弱性（CVE-2021-21972）に関する注意喚起（更新） Apache Tomcatの脆弱性（CVE-2020-9484）に関する注意喚起（更新） Microsoft Exchange Serverの複数の脆弱性に関する注意喚起（公開） FileZenの脆弱性（CVE-2021-20655）に関する注意喚起（更新） Microsoft Exchange Serverの複数の脆弱性に関する注意喚起（更新） 2021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（公開） 複数のBIG-IP製品の脆弱性（CVE-2021-22986）に関する注意喚起（公開） OpenSSLの脆弱性（CVE-2021-3450、CVE-2021-3449）に関する注意喚起（公開） OpenSSLの脆弱性（CVE-2021-3450、CVE-2021-3449）に関する注意喚起（更新）
2021年4月	VMware vRealize Operations Managerなどの複数の脆弱性に関する注意喚起（公開） 2021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（公開） Trend Micro Apex One,Apex One SaaS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-2020-24557）に関する注意喚起（公開） Pulse Connect Secureの脆弱性（CVE-2021-22893）に関する注意喚起（公開） 2021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（公開） Pulse Connect Secureの脆弱性（CVE-2021-22893）に関する注意喚起（更新） FileZenの脆弱性（CVE-2021-20655）に関する注意喚起（更新） ISC BIND 9の複数の脆弱性に関する注意喚起（公開）
2021年5月	Pulse Connect Secureの脆弱性（CVE-2021-22893）に関する注意喚起（更新） EC-CUBEのクロスサイトスクリプティングの脆弱性（CVE-2021-20717）に関する注意喚起（公開） 2021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（公開） Adobe AcrobatおよびReaderの脆弱性（APSB21-29）に関する注意喚起（公開） VMware vCenter Serverの複数の脆弱性（CVE-2021-21985、CVE-2021-21986）に関する注意喚起（公開）
2021年6月	VMware vCenter Serverの複数の脆弱性（CVE-2021-21985、CVE-2021-21986）に関する注意喚起（更新） 2021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（公開） Adobe AcrobatおよびReaderの脆弱性（APSB21-37）に関する注意喚起（公開）

	Adobe Acrobat および Reader の脆弱性（APSB21-37）に関する注意喚起（更新） 複数の EC-CUBE 3.0 系用プラグインにおけるクロスサイトスクリプティングの脆弱性に関する注意喚起（公開）
2021 年 7 月	Windows の印刷スプーラーの脆弱性（CVE-2021-34527）に関する注意喚起（公開） Windows の印刷スプーラーの脆弱性（CVE-2021-34527）に関する注意喚起（更新） Windows の印刷スプーラーの脆弱性（CVE-2021-34527）に関する注意喚起（更新） Windows の印刷スプーラーの脆弱性（CVE-2021-34527）に関する注意喚起（更新） 2021 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（公開） Adobe Acrobat および Reader の脆弱性（APSB21-51）に関する注意喚起（公開） 2021 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（公開） 複数のトレンドマイクロ製企業向けエンドポイントセキュリティ製品の脆弱性に関する注意喚起（公開）
2021 年 8 月	2021 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（公開） ISC BIND 9 の脆弱性（CVE-2021-25218）に関する注意喚起（公開） OpenSSL の脆弱性（CVE-2021-3711、CVE-2021-3712）に関する注意喚起（公開）
2021 年 9 月	Confluence Server および Data Center の脆弱性（CVE-2021-26084）に関する注意喚起（公開） Confluence Server および Data Center の脆弱性（CVE-2021-26084）に関する注意喚起（更新） Microsoft MSHTML の脆弱性（CVE-2021-40444）に関する注意喚起（公開） Microsoft MSHTML の脆弱性（CVE-2021-40444）に関する注意喚起（更新） Ghostscript の任意のコマンド実行が可能な脆弱性（CVE-2021-3781）に関する注意喚起（公開） 2021 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（公開） Adobe Acrobat および Reader の脆弱性（APSB21-55）に関する注意喚起（公開） Microsoft MSHTML の脆弱性（CVE-2021-40444）に関する注意喚起（更新） 2021 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（更新） Ghostscript の任意のコマンド実行が可能な脆弱性（CVE-2021-3781）に関する注意喚起（更新）
2021 年 10 月	SonicWall 製の SMA100 シリーズの脆弱性（CVE-2021-20034）に関する注意喚起（公開） Apache HTTP Server のパストラバーサルの脆弱性（CVE-2021-41773）に関する注意喚起（公開） Apache HTTP Server のパストラバーサルの脆弱性（CVE-2021-41773）に関する注意喚起（更新） 2021 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（公開）

	Adobe Acrobat および Reader の脆弱性（APSB21-104）に関する注意喚起（公開） Movable Type の XMLRPC API における脆弱性（CVE-2021-20837）に関する注意喚起（公開） 2021 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（公開）
2021 年 11 月	Movable Type の XMLRPC API における脆弱性（CVE-2021-20837）に関する注意喚起（更新） Movable Type の XMLRPC API における脆弱性（CVE-2021-20837）に関する注意喚起（更新） 2021 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（公開） Web メールサービスのアカウントを標的としたフィッシングに関する注意喚起（公開） Movable Type の XMLRPC API における脆弱性（CVE-2021-20837）に関する注意喚起（更新）
2021 年 12 月	Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起（公開） Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起（更新） Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起（更新） 2021 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（公開） Movable Type の XMLRPC API における脆弱性（CVE-2021-20837）に関する注意喚起（更新） Movable Type の XMLRPC API における脆弱性（CVE-2021-20837）に関する注意喚起（更新） Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起（更新） Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起（更新）

（２） 活動概要（報告状況等の公表）

発行日：2021/1/21［2020 年 10 月 1 日～2020 年 12 月 31 日］
発行日：2021/4/15［2021 年 1 月 1 日～2021 年 3 月 31 日］
発行日：2021/7/15［2021 年 4 月 1 日～2021 年 6 月 30 日］
発行日：2021/10/14[2021 年 7 月 1 日～2021 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］398 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５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
- サイバーフィジカルセキュリティ技術の研究開発

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３年12月６日から令和４年1月21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。

パスロジ株式会社

(2)　調査

警察庁が令和３年８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（14大学、23件）

東京理科大学（２件）
京都大学（３件）
岩手大学
東北工業大学
神奈川工科大学
東京電機大学
創価大学
中央大学（３件）
日本大学（４件）
金沢大学
中京大学
名古屋大学（２件）
立命館大学
福岡大学

イ　企業（５社、９件）

ソースネクスト株式会社
キャノン株式会社（４件）
富士電機株式会社（２件）
株式会社ネクストジェン
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248校、企業1,595社の計1,843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　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　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～令和2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、令和2年度までの延長を決定。

（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大規模・長期実証実験

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
（https://www.nict.go.jp/collabo/commission/k_190.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　侵入検知・防御技術、ぜい弱性対策技術

テーマ名　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

開発年度　平成30年度～令和3年度

実施主体　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）

法人番号　8011101028104(東日本電信電話株式会社)、4010405001654（学校法人慶應義塾）他

背景、目的

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。

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。

研究開発状況（概要）

平成30年度から研究開発を開始。

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。

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
（https://www.nict.go.jp/collabo/commission/k_195.html）
電話 042－327－6011

将来の方向性

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。

対象技術　インシデント分析技術

テーマ名　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

開発年度　令和元年度～令和2年度

実施主体　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）
法人番号　3290005003743（国立大学法人九州大学）、5011105000953（学校法人早稲田大学）他

背景、目的

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。

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。

研究開発状況（概要）

令和元年度から以下の研究開発を開始。

（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

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
（https://www.nict.go.jp/collabo/commission/k_21601.html）
電話 042－327－6011

将来の方向性

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。

対象技術　その他アクセス制御機能に関する技術、高度認証技術

テーマ名　サイバーフィジカルセキュリティ技術の研究開発

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

サイバー空間（仮想空間）とフィジカル空間（現実空間）が高度に融合した社会では、サイバー空間、フィジカル空間、両者の境界における攻撃、それらを組み合わせた攻撃が存在する。これらの攻撃を防ぐアクセス制御技術として、高い安全性と効率性（速度、メモリ等）を両立する暗号技術の研究開発を行う。

研究開発状況（概要）

複雑なアクセス制御を柔軟に実現する高機能暗号技術や、暗号化した状態で検索や計算を行う技術（秘匿データベースについては企業との連携で実用化）、匿名認証技術、さらにはIoT機器との通信のセキュリティを高める軽量暗号技術等の提案を行っている。

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 産業技術総合研究所 サイバーフィジカルセキュリティ研究センター
TEL: 03-3599-8001（代表）
URL:https://www.cpsec.aist.go.jp/

将来の方向性

データの授受に関わるハードウェア、ソフトウェアのセキュリティ対策技術と組み合わせることで、サイバーフィジカルシステム全体のセキュリティ測定、強化、保証する技術を確立していく。

（別添２）

企業名（及び略称）　パスロジ株式会社 法人番号　8010001091039	
代表者氏名　小川 秀治	
所在地（郵便番号及び住所）東京都千代田区神田神保町一丁目６番地１　タキイ東京ビル７階	
関連部署名及び電話番号　ログインプロテクト担当窓口 03-5283-2263	
ＵＲＬ　https://www.passlogy.com/	
対象技術	技術開発状況
高度認証技術（ログインプロテクト） 平成26年度から研究開発を開始	インターネット上サービスなどへのログイン可能な時間を極限まで減らすことで、認証のセキュリティ強度を高める技術を開発。 これまでの認証の仕組みとの最大の相違は「認証を受け付けない状態が標準状態」であり、その状態においては、ログインフォームに対していかなるパラメータ（たとえ正解であっても）を送信してもシャットアウトすること。 正規の利用者がログインする際には、スマートフォンアプリをワンタップし、「これからログインする」という合図をサービスに送信し、サービス側は、合図を受け取ってから1分間だけ、ログインを待ち受ける状態になる。 この間に利用者はいつも通りのログイン操作で安全な認証を経て、ログイン可能となるので、不正アクセス及びアカウントロック攻撃 の被害に遭うリスクを低減することができる。 **本技術情報の詳細**：https://www.passlogy.com/pdf/loginprotect_202201.pdf

（別添３）

ア　大学

企業・大学名	東京理科大学
代表者名	本間　芳和
所在地	162-8601 東京都新宿区神楽坂1-3
窓口部署名	研究戦略・産学連携センター　企画管理部門
電話番号	03-5228-7440
ホームページのURL	https://www.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: クリプトボックス 開発元(メーカー名等): 株式会社クリプト・ベーシック 開発国: 日本 価格: 50万円 発売時期: 2012年4月1日～ 出荷数: 2	独自の鍵共有プロトコルと共通鍵暗号方式により従来と比較して10倍以上の鍵長を持つ暗号通信をもとに，強力なVPNを構築できる.

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	東京理科大学
代表者名	本間　芳和
所在地	〒162-8601 東京都新宿区神楽坂1-3
窓口部署名	研究戦略・産学連携センター　企画管理部門
電話番号	03-5228-7440
関連部門名	認証技術
ホームページのURL	https://www.tus.ac.jp
研究説明のURL	https://wakasapo.nedo.go.jp/seeds/seeds-0246/
対象技術	技術の概要・特徴など
研究開発名称： PDI認証 研究開発国： 日本 研究開発時期： 2016年4月1日～	理論及び研究実装，POC用プロトタイプが完成している． 現在，サービス開始を目指し，サーバー安定稼働，API整備を進めている．

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	

企業・大学名	京都大学学術情報メディアセンター
代表者名	センター長　岡部　寿男
所在地	606-8501 京都府京都市左京区吉田本町
窓口部署名	情報部　情報推進課　総務掛
電話番号	075-753-7400
ホームページのURL	https://www.media.kyoto-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: eduroam JP 開発元(メーカー名等): 国立情報学研究所 開発国: 日本（欧州と共同開発） 価格: 無料 発売時期: 2006年8月～ 出荷数: 国内310機関	教育、研究機関で提供されるキャンパス無線LANを相互に安全にローミングで利用できるようにする国際的な認証連携のしくみ　www.eduroam.jp

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	京都大学学術情報メディアセンター
代表者名	センター長　岡部　寿男
所在地	606-8501 京都府京都市左京区吉田本町
窓口部署名	情報部　情報推進課　総務掛
電話番号	075-753-7400
ホームページのURL	https://www.media.kyoto-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: 学術認証フェデレーション GakuNin 開発元(メーカー名等): 国立情報学研究所 開発国: 日本 価格: 無料 発売時期: 2009年4月～ 出荷数: 大学等258機関、サービス提供機関188	学術eリソースを利用する大学等と学術eリソースを提供する出社等が相互に認証連携を行うための国際的なしくみ www.gakunin.jp

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	京都大学学術情報メディアセンター
代表者名	センター長　岡部　寿男
所在地	〒606-8501 京都府京都市左京区吉田本町
窓口部署名	情報部　情報推進課　総務掛
電話番号	075-753-7400
関連部門名	ネットワーク研究部門
ホームページのURL	https://www.media.kyoto-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： 対話的に通信制御が可能なマルウェア解析システム 研究開発国： 日本 研究開発時期： 2020年4月～	マルウェア解析のためのサンドボックス上での通信制御の仕組みとして、対話的に制御が可能なシステムを開発している。

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	

企業・大学名	国立大学法人岩手大学
代表者名	学長　小川　智
所在地	〒020-8550 岩手県盛岡市上田三丁目１８番８号
窓口部署名	理工学部事務部
電話番号	019-621-6305
関連部門名	理工学部システム創成工学科知能・メディア情報コース
ホームページのURL	https://www.iwate-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： ウイルスの検出・分類に関する研究 研究開発国： 日本 研究開発時期： 2016年4月～	ウイルスの表層あるいは動的解析結果を利用した，機械学習による検出・分類手法の研究を行っている．

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	

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	https://www.tohtech.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： 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 研究開発国： 日本 研究開発時期： 2015年4月～	基本要素のモデル化と基本要件の分析が完了しており，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プロタイプ実装を開発して，提案の概念実証と基本的実現性を確認している. 現在は，開発したプロトタイプ実装をベースとして実装の改良を進めるとともに，実用性に関する検討のため様々なIoT デバイスを対象とした実験を進めようとしている

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	○

企業・大学名	神奈川工科大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報学部
ホームページのURL	
研究説明のURL	https://ipsj.ixsq.nii.ac.jp/ej/index.php?active_action=repository_view_main_item_detail&page_id=13&block_id=8&item_id=208504&item_no=1 https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=211007&item_no=1&page_id=13&block_id=8
対象技術	技術の概要・特徴など
研究開発名称： IoTマルウェアの解析技術の研究開発 研究開発国： 日本 研究開発時期： 2019年10月1日～2022年3月1日	IoTマルウェアの解析の要となるライブラリ関数の特定が完了した。今後はライブラリ関数の情報を活用して、関数のトレースによる動的解析技術やIoTマルウェアの検知・亜種分類の研究開発を行う予定である。

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	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	https://www.dendai.ac.jp/crc/
研究説明のURL	http://www.lab.ine.aj.dendai.ac.jp/wordpress/
対象技術	技術の概要・特徴など
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 研究開発国： 日本 研究開発時期： 2007年3月6日～2021年12月31日	秘密電子メール、秘密映像伝達技術並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、技術展開が出来るレベルに達している。

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	○

企業・大学名	創価大学　理工学部　情報システム工学科
代表者名	
所在地	〒192-0003 東京都八王子市丹木町1-236
窓口部署名	理工学部事務室
電話番号	042-691-9400
関連部門名	創価大学　理工学部　情報システム工学科
ホームページのURL	www.soka.ac.jp/science/infosys/
研究説明のURL	www.soka.ac.jp/science/infosys
対象技術	技術の概要・特徴など
研究開発名称： サイバーフィジカルシステムのセキュリティに関する研究 研究開発国： 日本 研究開発時期： 2017年4月1日～2023年3月31日	大学の研究室内での研究であり、実用等商品化は考えていない

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	学校法人中央大学
代表者名	大村　雅彦
所在地	〒192-0393 東京都八王子市東中野７４２－１
窓口部署名	AI・データサイエンスセンター
電話番号	03-3817-7463
関連部門名	国際情報学部
ホームページのURL	https://www.chuo-u.ac.jp/aboutus/efforts/ai_and_ds/
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： SDNにおける文脈型動的セキュリティプロトコル 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	学校法人中央大学
代表者名	大村　雅彦
所在地	〒192-0393 東京都八王子市東中野７４２－１
窓口部署名	AI・データサイエンスセンター
電話番号	03-3817-7463
関連部門名	研究開発機構（ユニット代表者：趙　晋輝）
ホームページのURL	https://www.chuo-u.ac.jp/aboutus/efforts/ai_and_ds/
研究説明のURL	ありません
対象技術	技術の概要・特徴など
研究開発名称： 新常態環境下の情報セキュリティに関する総合的研究（ユニット名） 研究開発国： 日本 研究開発時期： 2019年4月1日～2022年3月31日	企業秘密に関係するため開示は出来ません

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	学校法人中央大学
代表者名	大村　雅彦
所在地	〒192-0393 東京都八王子市東中野７４２－１
窓口部署名	AI・データサイエンスセンター
電話番号	03-3817-7463
関連部門名	国際情報学部
ホームページのURL	https://www.chuo-u.ac.jp/aboutus/efforts/ai_and_ds/
研究説明のURL	http://www.iperc.uec.ac.jp/datafile/annualreport/iPERC2019HP.pdf
対象技術	技術の概要・特徴など
研究開発名称： 産業用インターネットオブシングス（Industrial Internet of Things: IIoT)機器・システムに対する遠隔セキュリティ検証手法 研究開発国： 日本 研究開発時期： 2019年4月1日～	制御システムの模擬プラントにおいて評価を進める中で、実用化する上での課題に対処している。

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	

企業・大学名	日本大学
代表者名	
所在地	〒102-8275 東京都千代田区九段南4-8-24
窓口部署名	研究推進部 研究事務課
電話番号	03-5275-8137
関連部門名	理工学部応用情報化学科
ホームページのURL	http://www.nihon-u.ac.jp/
研究説明のURL	https://53lab.jp/
対象技術	技術の概要・特徴など
研究開発名称： 生体から得られる電磁気情報を用いた個人認証システム 研究開発国： 日本 研究開発時期： 2016年12月1日～	実験用のシステムを構築し、有効性の検証を行っている。

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	

企業・大学名	日本大学
代表者名	
所在地	〒102-8275 東京都千代田区九段南4-8-24
窓口部署名	研究推進部 研究事務課
電話番号	03-5275-8137
関連部門名	理工学部応用情報工学科
ホームページのURL	http://www.nihon-u.ac.jp/
研究説明のURL	https://53lab.jp/
対象技術	技術の概要・特徴など
研究開発名称： ブロックチェーン技術を用いた単一医療機関向け診療記録システム 研究開発国： 日本 研究開発時期： 2017年12月1日～	実験用のシステムを構築し、有効性の検証を行っている。

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	

企業・大学名	日本大学
代表者名	
所在地	〒102-8275 東京都千代田区九段南4-8-24
窓口部署名	研究推進部 研究事務課
電話番号	03-5275-8137
関連部門名	理工学部応用情報工学科
ホームページのURL	http://www.nihon-u.ac.jp/
研究説明のURL	https://53lab.jp/
対象技術	技術の概要・特徴など
研究開発名称： 標的型メール対策訓練支援システム 研究開発国： 日本 研究開発時期： 2017年12月15日～	実験用のシステムを構築し、有効性の検証を行っている。

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	

企業・大学名	日本大学
代表者名	
所在地	〒102-8275 東京都千代田区九段南4-8-24
窓口部署名	研究推進部 研究事務課
電話番号	03-5275-8137
関連部門名	理工学部応用情報工学科
ホームページのURL	http://www.nihon-u.ac.jp/
研究説明のURL	https://53lab.jp/
対象技術	技術の概要・特徴など
研究開発名称： デジタルフォレンジック技術の学習支援システム 研究開発国： 日本 研究開発時期： 2018年9月1日～	実験用のシステムを構築し、有効性の検証を行っている。

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	

企業・大学名	国立大学法人金沢大学
代表者名	学長　　山崎　光悦
所在地	〒〒920－1192 石川県金沢市角間町
窓口部署名	研究・社会共創推進部研究推進課研究推進総務係
電話番号	076-264-5230
関連部門名	学術メディア創成センター
ホームページのURL	https://www.kanazawa-u.ac.jp/
研究説明のURL	ホームページでは公開しない
対象技術	技術の概要・特徴など
研究開発名称： Raspberry Gate 研究開発国： 日本 研究開発時期： 2011年4月1日～	組み込み機器のセキュリティ研究の一環としてアクセス制御の技術開発も行っている

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	

企業・大学名	中京大学
代表者名	
所在地	〒466-8666 名古屋市昭和区八事本町１０１－２
窓口部署名	学園経営戦略部
電話番号	052-835-7138
関連部門名	中京大学工学部
ホームページのURL	https://www.chukyo-u.ac.jp/
研究説明のURL	http://www.e-ontap.com/blog/?date=20210331
対象技術	技術の概要・特徴など
研究開発名称： 隠れオープンリゾルバスキャナ 研究開発国： 日本 研究開発時期： 2021年3月1日～	試験運用中。すでに数千の脆弱なネットワークを発見し、JPCERT/CC へ報告している。商用化の計画は無し。研究発表は 1,2 年中に計画。

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	国立大学法人東海国立大学機構名古屋大学
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研究部門 基盤ネットワーク研究G
ホームページのURL	
研究説明のURL	https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/network_security.html https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/cyber_security.html https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/network.html
対象技術	技術の概要・特徴など
研究開発名称： （特に名称をつけていない） 研究開発国： 日本 研究開発時期：	大学における継続的な研究であり、特に期間を区切って研究開発しているわけではない。

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	国立大学法人東海国立大学機構名古屋大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	研究開発機構（ユニット代表者：趙　晋輝）
ホームページのURL	
研究説明のURL	ありません
対象技術	技術の概要・特徴など
研究開発名称： 新常態環境下の情報セキュリティに関する総合的研究（ユニット名） 研究開発国： 日本 研究開発時期： 2019年4月1日～2022年3月31日	企業秘密に関係するため開示は出来ません

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	学校法人立命館（立命館大学）
代表者名	森島朋三
所在地	〒604-8418 京都府京都市中京区西ノ京東栂尾町８番地
窓口部署名	BKCリサーチオフィス
電話番号	077-561-2802
関連部門名	情報理工学部
ホームページのURL	http://www.ritsumei.ac.jp/
研究説明のURL	https://www.asl.cs.ritsumei.ac.jp/研究プロジェクト:salvia
対象技術	技術の概要・特徴など
研究開発名称： 情報漏洩を防止するオペレーティングシステム 研究開発国： 日本 研究開発時期： 2003年4月1日～	情報漏洩を防止する基盤ソフトウェアというコンセプトに基づき，オーバヘッド，実現可能性，機能的限界などの各視点から，複数の実現手法について検討・開発を進めている．

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	○

企業・大学名	学校法人福岡大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	福岡大学情報基盤センター中國研究室
ホームページのURL	
研究説明のURL	なし
対象技術	技術の概要・特徴など
研究開発名称： キーボード入力のタイミングを用いた生体認証 研究開発国： 日本 研究開発時期： 2016年9月1日～2022年3月31日	現段階では少数の被験者の協力による認証精度を確認している。 極めて高い認証精度を確認しており、近日中に多くの被験者を用いて、認認証精度を検証する計画である。 現在は、国内のセキュリティ製品を開発するメーカーと共同研究開発を推進することを協議しており、同メーカーから日本国内に向けて販売することを目指す。

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	ソースネクスト株式会社
代表者名	代表取締役社長 兼 COO 小嶋智彰
所在地	105-7133 東京都港区東新橋1-5-2　汐留シティセンター33階
窓口部署名	
電話番号	
ホームページのURL	https://sourcenext.co.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名: ZERO ウイルスセキュリティ 開発元(メーカー名等): K7 Computing Pvt Ltd. 開発国: インド 価格: 1,980円・税込（1台用） 発売時期: 2003年11月14日～ 出荷数: 累計1000万台以上	「ZERO ウイルスセキュリティ」は、2006年より更新料0円で発売している製品。 「ウイルスセキュリティ」そのものは2003年の発売です。 「ウイルスセキュリティ」のエントリー数はのべ1000万台を突破しています。

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	キヤノン株式会社
代表者名	御手洗冨士夫
所在地	146-8501 東京都大田区下丸子3-30-2
窓口部署名	
電話番号	03-3758-2111
ホームページのURL	https://global.canon
製品説明のURL	
対象技術	技術の概要・特徴など
製品名: imageRUNNER ADVANCE/DX シリーズ 開発元(メーカー名等): キヤノン株式会社 開発国: 日本 価格: 本体標準価格 67万円～500万円 発売時期: 2016年1月1日～ 出荷数:	弊社製品はオフィスにおけるネットワーク事務機器であり、顧客のオフィスネットワークインフラに接続され顧客情報が流通する為、セキュリティ脅威として、悪意や誤用による情報漏洩、他の情報機器へ攻撃踏み台としての悪用などの可能性に対して、高度な暗号化による盗聴防止、 ユーザ認証機能による権限のある情報参照への認可、 ファームウェアの改ざん防止・検知など、セキュリティに対して万全の備えを有している。

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	○

企業・大学名	キヤノン株式会社
代表者名	御手洗冨士夫
所在地	〒146-8501 東京都大田区下丸子3-30-2
窓口部署名	
電話番号	03-3758-2111
関連部門名	デジタルビジネスプラットフォーム開発本部
ホームページのURL	https://global.canon
研究説明のURL	外部公開していません。
対象技術	技術の概要・特徴など
研究開発名称： 改ざん検知・復旧技術開発 研究開発国： 日本 研究開発時期： 2017年5月～2022年1月	改ざん検知、復旧の順に開発を進めております。改ざん検知については商用化済みでして、復旧について商用化を目指して開発を進めている状況です。

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	キヤノン株式会社
代表者名	御手洗冨士夫
所在地	〒146-8501 東京都大田区下丸子3-30-2
窓口部署名	
電話番号	03-3758-2111
関連部門名	デジタルビジネスプラットフォーム開発本部
ホームページのURL	https://global.canon
研究説明のURL	外部公開していません。
対象技術	技術の概要・特徴など
研究開発名称： 無線LANセキュリティ技術開発 研究開発国： 日本 研究開発時期： 2020年6月～2022年6月	無線LANセキュリティ技術開発として、1年以内の商用化を目指して、ハードウェアおよびソフトウェアの開発を進めております。

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	キヤノン株式会社
代表者名	御手洗冨士夫
所在地	〒146-8501 東京都大田区下丸子3-30-2
窓口部署名	
電話番号	03-3758-2111
関連部門名	デジタルビジネスプラットフォーム開発本部
ホームページのURL	https://global.canon
研究説明のURL	外部公開していません。
対象技術	技術の概要・特徴など
研究開発名称： Canon ID(コンシューマ向け認証認可基盤) 研究開発国： 日本 研究開発時期： 2015年1月～2022年12月	コンシューマ向け認証認可基盤として開発を進めております。Canon IDとして商用化済みでして、現在は、Canon IDに対して多要素認証の導入などセキュリティを向上する機能を提供するべく開発を進めている状況です。

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	富士電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	https://www.fujielectric.co.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名: IoTプラットフォーム 開発元(メーカー名等): 富士電機株式会社 開発国: 日本 価格: 発売時期: 2018年9月1日～ 出荷数:	当社顧客サイトに設置されるエッジコントローラと、エッジコントローラにより収集したデータに基づきサービスを提供するクラウドから構成される。 提供サービスにはエネルギーマネジメント、稼働監視などが含まれる。

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	富士電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	技術開発本部　デジタルイノベーション研究所
ホームページのURL	https://www.fujielectric.co.jp/
研究説明のURL	https://www.fujielectric.co.jp/about/technology/fundamental/embedded_equipment.html
対象技術	技術の概要・特徴など
研究開発名称： 組込機器のセキュリティ技術 研究開発国： 日本 研究開発時期： 2019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	株式会社ネクストジェン
代表者名	大西　新二
所在地	108-0072 東京都港区白金1-27-6　白金高輪ステーションビル6F
窓口部署名	
電話番号	03-5793-3230
ホームページのURL	https://www.nextgen.co.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名: VOIPセキュリティ診断サービス 開発元(メーカー名等): 株式会社ネクストジェン 開発国: 日本 価格: 実施内容による 発売時期: 2007年～ 出荷数: 200機器程度の診断実績	VIOP音声網に対するセキュリティ診断サービスです。新たな攻撃ツールや手法について継続的な調査を行っており、診断サービスでは、これらをもとに机上検討及び模擬攻撃を実施し、なりすましや改ざん、盗聴といった音声網へのリスクを可視化します。固定電話やモバイルなど通信事業者や、クラウドPBXサービス事業者、またはこれらに設備を導入するベンダが主な顧客です。国内の大手通信事業者が主な顧客ですが、詳細は当社HP（下記）をご覧ください。 https://www.nextgen.co.jp/solution/voip/service/sipvoip.html

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6-4　ニチレイ明石町ビル
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	https://www.asgent.co.jp/
研究説明のURL	https://www.asgent.co.jp/press/releases/2014/20140117-000373.html
対象技術	技術の概要・特徴など
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 研究開発国： 日本 研究開発時期： 2014年4月1日～継続中	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へ発信しています。

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	