令和７年３月13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６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６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

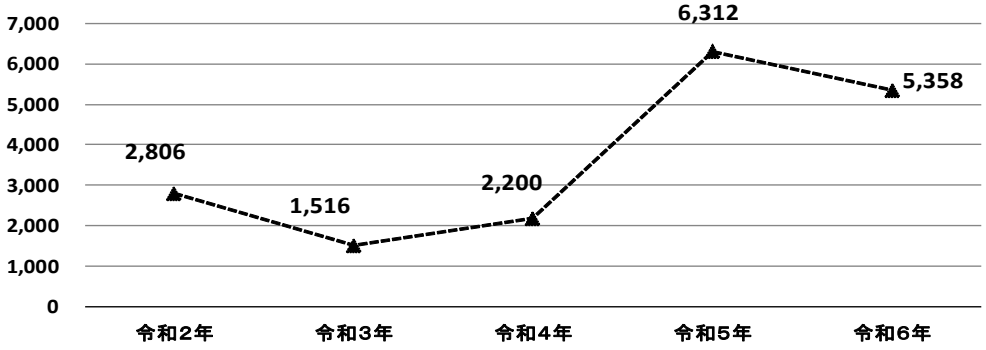
令和６年に都道府県警察から警察庁に報告がなされた不正アクセス行為の認知・検挙状況等は次のとおりである。

１　不正アクセス行為の認知状況

(1)　認知件数

令和６年における不正アクセス行為の認知件数[注1]は5,358件であり、前年（令和５年）と比べ、954件（約15.1%）減少した。

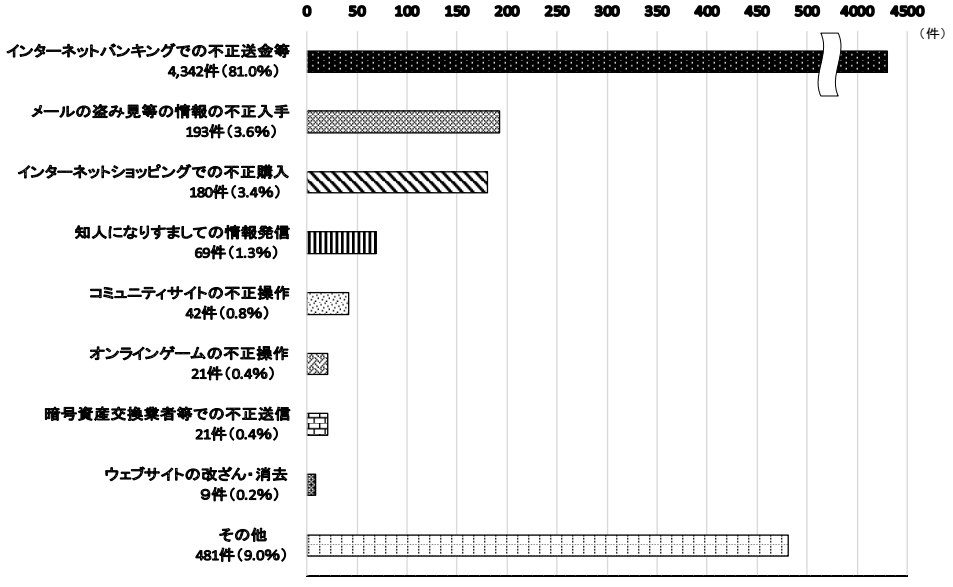
図１－１　不正アクセス行為の認知件数の推移（過去５年）



(2)　不正アクセス後の行為別の内訳

令和６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（4,342件）、次いで「メールの盗み見等の情報の不正入手」（193件）、「インターネットショッピングでの不正購入」（180件）の順となっている。

図１－２　令和６年における不正アクセス後の行為別認知件数



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行為の数をいう。

表１－１　不正アクセス後の行為別認知件数（過去５年）

区分＼年次	令和2年	令和3年	令和4年	令和5年	令和6年
インターネットバンキングでの不正送金等	1,847	693	1,096	5,598	4,342
メールの盗み見等の情報の不正入手	234	175	215	204	193
インターネットショッピングでの不正購入	172	349	227	93	180
知人になりすましての情報発信	26	71	50	33	69
コミュニティサイトの不正操作	46	49	34	65	42
オンラインゲームの不正操作	35	16	29	18	21
暗号資産交換業者等での不正送信	18	20	32	14	21
ウェブサイトの改ざん・消去	10	8	17	8	9
インターネットオークションの不正操作	6	4	0	3	0
その他	412	131	500	276	481
計	2,806	1,516	2,200	6,312	5,358

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６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563件・259人であり、前年（令和５年）と比べ、42件増加し、検挙人員は同数であった。

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533件・252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2]」が３件・２人、「識別符号提供（助長）行為[注3]」が11件・４人、「識別符号保管行為[注4]」が14件・９人、「識別符号不正要求行為[注5]」が２件・２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		令和2年	令和3年	令和4年	令和5年	令和6年
不正アクセス行為	検挙件数	585	408	491	487	533
	検挙事件数 [注6]	199	189	223	216	228
	検挙人員	216	227	243	248	252
識別符号取得行為	検挙件数	3	4	8	11	3
	検挙事件数	3	2	5	4	2
	検挙人員	3	2	5	8	2
識別符号提供(助長)行為	検挙件数	4	9	5	13	11
	検挙事件数	4	8	5	6	4
	検挙人員	4	8	5	10	4
識別符号保管行為	検挙件数	14	7	16	7	14
	検挙事件数	13	6	8	6	9
	検挙人員	13	6	8	6	9
識別符号不正要求行為	検挙件数	3	1	2	3	2
	検挙事件数	2	1	2	2	2
	検挙人員	5	1	2	2	2
計	検挙件数	609	429	522	521	563
	検挙事件数	207 (重複14)	195 (重複11)	237 (重複6)	221 (重複13)	232 (重複13)
	検挙人員	230 (重複11)	235 (重複9)	257 (重複6)	259 (重複15)	259 (重複10)

※　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2　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3　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。

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

注4　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5　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6　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６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7]」が511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		令和2年	令和3年	令和4年	令和5年	令和6年
識別符号窃用型	検挙件数	576	398	482	475	511
	検挙事件数	190	182	215	207	210
セキュリティ・ホール攻撃型	検挙件数	9	10	9	12	22
	検挙事件数	9	8	8	10	18
計	検挙件数	585	408	491	487	533
	検挙事件数	199	189 （重複1）	223	216 （重複1）	228

※　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7　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６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（105人）、次いで「14～19歳」（72人）、「30～39歳」（42人）の順となっている[注8]。

なお、令和６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9]、最年長の者は63歳であった。

図３－１　令和６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

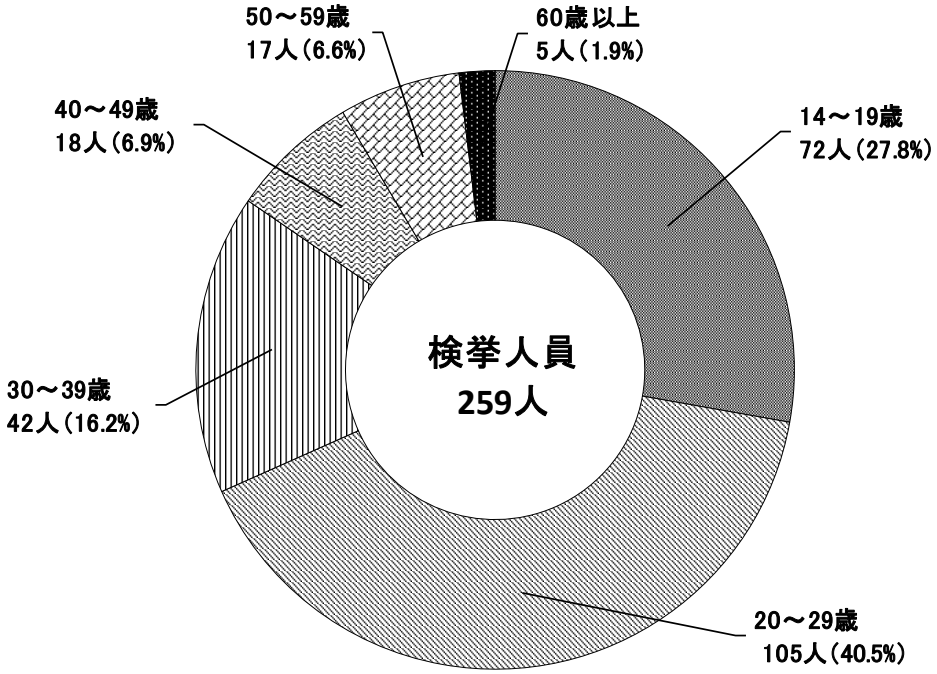


表３－１　年齢別被疑者数の推移（過去５年）

区分＼年次	令和2年	令和3年	令和4年	令和5年	令和6年
14～19歳	48	60	68	73	72
20～29歳	103	87	104	103	105
30～39歳	52	43	55	53	42
40～49歳	17	30	15	21	18
50～59歳	9	11	14	8	17
60歳以上	1	4	1	1	5
計	230	235	257	259	259

注8　このほか、不正アクセス禁止法違反で、14歳未満の少年18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9　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。

(2)　不正アクセス行為の手口別検挙件数

令和６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（511件）について、その手口別に内訳を見ると、「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（174件）、次いで「識別符号を知り得る立場にあった元従業員や知人等による犯行」（107件）の順となっており、前年（令和５年）と比べ、前者は約0.86倍、後者は約1.57倍となっている。

図３－２　令和６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

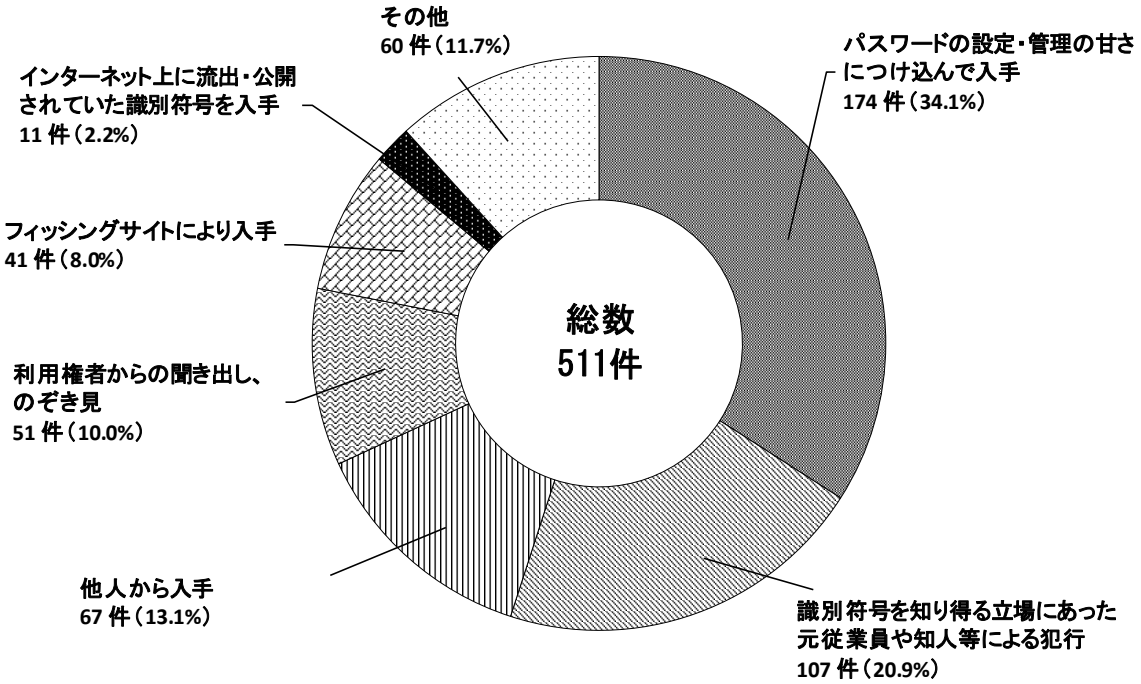


表３－２　不正アクセス行為の手口別検挙件数（過去５年）

区分＼年次	令和2年	令和3年	令和4年	令和5年	令和6年
識別符号窃用型	576	398	482	475	511
パスワードの設定・管理の甘さにつけ込んで入手	99	153	230	203	174
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	67	51	41	68	107
他人から入手	78	34	27	36	67
利用権者からの聞き出し、のぞき見	115	36	38	40	51
フィッシングサイトから入手	172	70	14	10	41
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	1	2	9	2	11
スパイウェア[注10]等のプログラムを使用して入手	3	0	0	2	0
その他	41	52	123	114	60
セキュリティ・ホール攻撃型	9	10	9	12	22

注10　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。

(3)　不正に利用されたサービス別検挙件数

令和６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（511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（221件）、次いで「コミュニティサイト」（108件）の順となっており、前年（令和５年）と比べ、前者は約2.70倍、後者は0.48倍となっている。

図３－３　令和６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

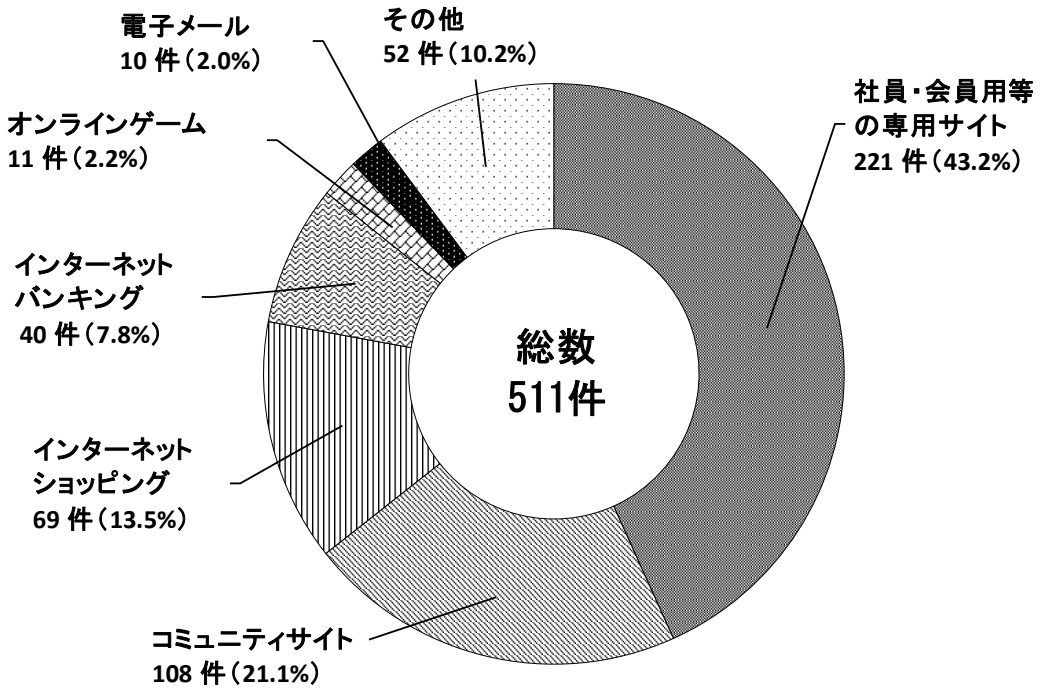


表３－３　不正アクセス行為（識別符号窃用型）により不正に利用されたサービス別検挙件数（過去５年）

区分＼年次	令和2年	令和3年	令和4年	令和5年	令和6年
社員・会員用等の専用サイト	174	75	104	82	221
コミュニティサイト	69	135	206	225	108
インターネットショッピング	36	38	26	35	69
インターネットバンキング	12	96	17	29	40
オンラインゲーム	19	9	27	9	11
電子メール	24	14	14	3	10
ウェブサイト公開サービス	1	4	8	0	0
インターネット接続サービス	1	0	1	0	0
インターネットオークション	1	0	0	0	0
その他	239	27	79	92	52
計	576	398	482	475	511

４　令和６年の主な検挙事例

(1)　会社員の男（37）は、令和４年11月、勤務先の名刺管理サービスの正規利用権者の識別符号を不正に取得し、令和５年２月、同識別符号を利用して名刺管理サービスに不正にログインするなどした。令和６年２月、男を不正アクセス禁止法違反（識別符号取得行為及び不正アクセス行為）で検挙した。

(2)　アルバイト従業員の男（21）は、令和５年５月から同年６月までの間、電気通信会社のメール配信ソフトの脆弱性を突き、同社のサーバコンピュータに不正プログラム（バックドア）を設置した上、同プログラムを利用して同サーバコンピュータに不正にログインした。令和６年10月、男を不正アクセス禁止法違反（不正アクセス行為）及び不正指令電磁的記録供用罪で検挙した。

(3)　無職の男（44）は、令和５年１月から同年２月までの間、会社員の男に指示し、不正に入手した他人の識別符号を使用して、インターネットバンキングに不正アクセスし、自らが管理する預金口座に不正送金させるなどした。令和６年７月、男を不正アクセス禁止法違反（不正アクセス行為）、電子計算機使用詐欺罪等で検挙した。

(4)　無職の男（22）は、令和５年６月、インターネット上で影響力を持つインフルエンサーに虚偽のキャッシュバックキャンペーンを宣伝させ、応募者から消費者金融サイトの識別符号を不正に入手し、同識別符号を利用して同サイトに不正アクセスした上、ＡＴＭから借入金を不正に引き出すなどした。令和６年１月、男を不正アクセス禁止法違反（不正アクセス行為）及び窃盗罪で検挙した。

(5)　無職の男（20）は、令和６年３月、正規のゲームアカウント売買サイトを偽装したフィッシングサイトを作成してインターネット上に公開し、複数の利用権者からオンラインゲームの識別符号を不正に取得した後、同識別符号を使用してオンラインゲームへ不正アクセスした。令和６年10月、男を不正アクセス禁止法違反（識別符号不正取得行為及び不正アクセス行為）及び電子計算機使用詐欺罪で検挙した。

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・パスワード等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11]や二経路認証[注12]を利用するなど、金融機関、ショッピングサイト、ゲーム会社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11　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からのアプリによる認証を追加する場合等がこれに当たる。

注12　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の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機器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、セキュリティパッチの適用やソフトウェアのバージョンアップを行うことなどにより、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・パスワード等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に加え、次世代認証技術（パスキー[注13]）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などについて、利用権者に対して注意喚起を行うとともに、自社のドメインの悪用を防止する観点で送信ドメイン認証技術（DMARC[注14]、SPF[注15]、DKIM[注16]）を導入する。

注13　パスキー：FIDO AllianceとWorld Wide Web Consortiumにより規格化されているパスワードが不要な認証技術。フィッシングサイト等の正規サイト以外のウェブサイトにおいては、認証が機能しないといった観点から認証技術の漏えいリスクを低減できる効果があるとされている。

注14　DMARC(Domain-based Message Authentication, Reporting, and Conformance)：SPF・DKIMの認証結果を利用し総合的に送信ドメイン認証を行う技術。受信したメールが正規の送信元から送られてきたかを検証できる技術の一つ。ドメイン管理者は、認証に失敗したメールの取扱いを送信側でポリシー（DMARC ポリシー）として宣言できる。これにより、なりすまされているメールは受け取らない、といった強いポリシーを受信側に伝えることができるようになる。

注15　SPF（Sender Policy Framework）：送信側のメールサーバのIPアドレスをDNSで宣言することにより、ネットワーク的に認証を実施する技術。

注16　DKIM（DomainKeys Identified Mail）：送信側のメールサーバで作成した電子署名により認証する技術。

（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６年（令和６年１月１日から令和６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 166 件（令和５年：243 件）であった（注２）。令和６年は令和５年と比べて、77 件（約 31.7%）減少した。

この届出された中には、被害の全貌把握や原因の特定に至っていないものも存在しており、当機構が把握できた範囲での内容となるが、届出で主に見受けられたものとして、VPN 装置の脆弱性やリモートデスクトッププロトコル（RDP）の設定不備を侵入経路としたランサムウェア攻撃(データを暗号化しない攻撃も含む)があった。そのほか、ウェブサイト（EC サイトを含む）の脆弱性を悪用した攻撃による改ざん被害、総当たり攻撃により、メールアカウントを乗っ取られたことによる不正メールの送信被害等が見られた。

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 407 件（令和５年：698 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 316 件（令和５年：512 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。

４件あり、ポートスキャンや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。

103 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：51 件
システムの設定不備を悪用した攻撃：34 件
パスワード推測（パスワードリスト攻撃等）：18 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。209 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：101 件
不正プログラムの埋め込み：65 件
資源利用(CPU 等のリソース不正使用)：31 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、８件（令和５年：４件）であった。

ウ その他
正規ユーザになりすましてのサービスの不正利用やソーシャルエンジニアリング、不審メール等である。83 件（令和５年：182 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：37 件
不審メール（スパムメール、フィッシングメール、SMS 等）：23 件
ソーシャルエンジニアリング：６件

(2) 原因別分類
166 件の届出のうち、実際に被害に遭った 132 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 141 件（令和５年：206 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）。
なお、届出される中には「原因不明」としているものが依然として多いことを確認している。これは攻撃手口の巧妙化や攻撃者に痕跡を削除されてしまうケースもあるほか、特定に必要となるログ等が適切に取得できていなかった等が推測される。
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：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）：33 件

ID、パスワード管理の不備：23 件

原因不明：25 件

(3) 電算機別分類

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：57 件

クライアント：37 件

ファイルサーバ：29 件

(4) 被害内容別分類

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 328 件（令和５年：486 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：90 件

不正プログラムの埋め込み：60 件

ファイルの書き換え：51 件

(5) 対策情報

令和６年においても、ランサムウェア攻撃による被害やウェブサイトの改ざん等による被害が依然として多く見られた。これらを含む、原因別で分類した 141 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 29.1%（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）」が約 23.4%（33 件）であり、この２つの項目で約 52.5%（74 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 16.3%（23 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、
・ VPN 装置やウェブサイト等に限らず、利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及び修正プログラムの適用
・ 管理、運用しているシステムの定期的な脆弱性診断の実施
・ 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、着実に脆弱性や設定不備を解消していくことや、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を勧める。また、前述したように、「原因不明」とする届出も多いことから、ログ取得の方法や取得する期間を見直す等のほか、自組織で調査が難しい場合は外部機関に対応を依頼する等して、なるべく調査完遂を目指すことを勧める。

さらに、正規アカウントの悪用を防ぐためのユーザ向け対策として、
・ 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を勧める。

また、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】
ランサムウェア対策に関しては、次を参照することを勧める。
・「ランサムウェア対策特設ページ」
https://www.ipa.go.jp/security/anshin/measures/ransom_tokusetsu.html
ウェブサイトの脆弱性を悪用した攻撃等の対策に関しては、次を参照することを勧める。
・「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/websecurity/sitecheck.html
・「安全なウェブサイトの作り方」
https://www.ipa.go.jp/security/vuln/websecurity/about.html
・「EC サイト構築・運用セキュリティガイドライン」
https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html
・「JVN (Japan Vulnerability Notes)」 ※脆弱性対策情報ポータルサイト
https://jvn.jp/
また、昨今の高度標的型攻撃の対策として、次も参照しておくことを勧める。
・「高度標的型攻撃」対策に向けたシステム設計ガイド

https://warp.da.ndl.go.jp/info:ndljp/pid/12446699/www.ipa.go.jp/security/vuln/newattack.html

【個人ユーザ向け】

個人ユーザに関しては、次を参照することを勧める。

「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/

「MyJVN」（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、下記ページを参照されたい。なお、IPA では影響度の高いセキュリティ上の問題を確認した際に、「重要なセキュリティ情報」を発信している。日々のセキュリティ対策の一環として、こちらも活用することを勧める。

「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６年（令和６年１月１日から令和６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 47,677 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 23,401 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 1,993 件の報告があった。

[1/1-3/31: 697 件、4/1-6/30: 689 件、7/1-9/30: 374 件、10/1-12/31: 233 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 246 件の報告があった。

[1/1-3/31: 57 件、4/1-6/30: 43 件、7/1-9/30: 93 件、10/1-12/31: 53 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 151 件の報告があった。

[1/1-3/31: 45 件、4/1-6/30: 45 件、7/1-9/30: 25 件、10/1-12/31: 36 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 18 件の報告があった。

[1/1-3/31: 2 件、4/1-6/30: 3 件、7/1-9/30: 9 件、10/1-12/31: 4 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 18,819 件の報告があった。
[1/1-3/31: 4,781 件、4/1-6/30: 5,025 件、7/1-9/30: 4,233 件、10/1-12/31: 4,780 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 0 件の報告があった。
[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 14 件の報告があった。
[1/1-3/31: 4 件、4/1-6/30: 2 件、7/1-9/30: 6 件、10/1-12/31: 2 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 2,160 件の報告があった。
[1/1-3/31: 503 件、4/1-6/30: 797 件、7/1-9/30: 407 件、10/1-12/31: 453 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]

公開日	注意喚起内容
2024 年 1 月	2024 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）
	Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起（公開）
	Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起（更新）
	2024 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）
	Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起（更新）
	Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起（更新）
2024 年 2 月	Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起（更新）
	Fortinet 製 FortiOS の境域外書き込みの脆弱性（CVE-2024-21762）に関する注意喚起（公開）
	Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起（更新）
	Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起（更新）
	2024 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（APSB24-07）に関する注意喚起（公開）
	Fortinet 製 FortiOS の境域外書き込みの脆弱性（CVE-2024-21762）に関する注意喚起（更新）
	Fortinet 製 FortiOS の境域外書き込みの脆弱性（CVE-2024-21762）に関する注意喚起（更新）
	Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起（更新）
2024 年 3 月	2024 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）
2024 年 4 月	2024 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）
	Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起（公開）
	Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起（更新）
	Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起（更新）
	Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起（更新）

	Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起（更新）
	Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起（更新）
	Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起（更新）
2024 年 5 月	2024 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（APSB24-29）に関する注意喚起（公開）
2024 年 6 月	2024 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）
	Operation Blotless 攻撃キャンペーンに関する注意喚起（公開）
2024 年 7 月	2024 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）
2024 年 8 月	Adobe Acrobat および Reader の脆弱性（APSB24-57）に関する注意喚起（公開）
	2024 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）
2024 年 9 月	2024 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）
	Adobe Acrobat および Reader の脆弱性（APSB24-70）に関する注意喚起（公開）
	2024 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）
2024 年 10 月	2024 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）
	Fortinet 製 FortiManager における重要な機能に対する認証の欠如の脆弱性（CVE-2024-47575）等に関する注意喚起（公開）
	Fortinet 製 FortiManager における重要な機能に対する認証の欠如の脆弱性（CVE-2024-47575）等に関する注意喚起（更新）
2024 年 11 月	Fortinet 製 FortiManager における重要な機能に対する認証の欠如の脆弱性（CVE-2024-47575）等に関する注意喚起（更新）
	2024 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）
	Fortinet 製 FortiManager における重要な機能に対する認証の欠如の

	脆弱性（CVE-2024-47575）等に関する注意喚起（更新）
	Palo Alto Networks 製 PAN-OS の管理インタフェースにおける複数の脆弱性（CVE-2024-0012、CVE-2024-9474）に関する注意喚起（公開）
	Palo Alto Networks 製 PAN-OS の管理インタフェースにおける複数の脆弱性（CVE-2024-0012、CVE-2024-9474）に関する注意喚起（更新）
2024 年 12 月	Adobe Acrobat および Reader の脆弱性（APSB24-92）に関する注意喚起（公開）
	2024 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）

（２） 活動概要（報告状況等の公表）

発行日：2024/1/18［2023 年 10 月 1 日～2023 年 12 月 31 日］
発行日：2024/4/18［2024 年 1 月 1 日～2024 年 3 月 31 日］
発行日：2024/7/18［2024 年 4 月 1 日～2024 年 6 月 30 日］
発行日：2024/10/17[2024 年 7 月 1 日～2024 年 9 月 30 日］

（３） JPCERT/CC レポート

［発行件数］52 件
［脆弱性情報の発行件数］470 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

警察庁、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６件であり、その研究開発の概要は、別添１のとおりである。

- 生体認証を用いたアクセス制御機能利用製品の耐偽造能力評価・検証技術
- 超多数・多種移動体による人流・物流のためのダイナミックセキュアネットワークの研究
- 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
- サイバーフィジカルセキュリティ技術の研究開発
- サイバー空間の状況把握・防御技術の向上及び共通基盤の整備

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６年12月10日から令和７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ところ、提案は０件であった。

(2)　調査

警察庁が令和６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　大学等（15大学等、22件）

愛知工業大学
公立大学法人大阪
北九州市立大学
岐阜大学（２件）
東北工業大学
東京情報大学
名古屋大学
日本文理大学
日本大学（４件）
福岡大学（２件）
前橋工科大学
明星大学（３件）
横浜国立大学
琉球大学
和歌山大学

イ　企業（２社、３件）

株式会社アイ・エス・ビー
株式会社ソリトンシステムズ（２件）

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285校、企業1,599社の計1,884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（会社四季報）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　その他アクセス制御機能に関する技術

テーマ名　生体認証を用いたアクセス制御機能利用製品の耐偽造能力評価・検証技術

開発年度　令和６年度

実施主体　株式会社ＦＦＲＩセキュリティ（警察大学校が実施する委託研究の委託先）

法人番号　3011101046226

背景、目的

スマートフォン等モバイル機器は、個人に関する重要な情報の多くを記録しており、機器の紛失・盗難等への対策のため、今日では、生体認証によるロック機能が普及している。一方で、生体認証機能の安全性については、一般人が客観的に把握することは難しく、ひとたび特異な事例に基づく脅威が喧伝された場合、事後、関係者がその風評を払拭するためには、大きな努力を要する。また、生成AIによるなりすましの脅威も、現実のものとなりつつあり、画像生成AIの進展を踏まえれば、生体認証一般に対する脅威として、対抗技術開発の検討が必要である。

研究開発状況（概要）

令和５年度研究成果物である評価手法を、警察大学校が保有するモバイル機器に対して適用し、生体認証技術（指紋・顔画像）を利用するロック機能に関する耐偽造能力の実態を把握する。

詳細の入手方法（関連部署名及びその連絡先）

警察大学校　サイバーセキュリティ対策研究・研修センター 解析研究室
電話　042-354-3550

将来の方向性

把握した耐偽造能力の実態に基づき、利用者への注意喚起や製造事業者等への情報提供等を通じて安全性の高い生体認証技術の実装・普及を促す。

対象技術　高度認証技術

テーマ名　超多数・多種移動体による人流・物流のためのダイナミックセキュアネットワークの研究

開発年度　令和３年度～令和５年度

実施主体　ジャパンデータコム株式会社、学校法人早稲田大学

法人番号　7010401014418（ジャパンデータコム株式会社）、5011105000953（学校法人早稲田大学）

背景、目的

Beyond 5G/6Gの時代には、超多数・多種な貨物ドローン等の移動体の密な空間での協調稼働による時空間の有効活用が期待され、多数の移動体間でのセキュリティを確保し周波数資源を節約した上での高頻度・低遅延な相互通信が求められる。

研究開発状況（概要）

通信効率性の高い認証方法、柔軟性が高く検証可能な属性提示方法および信頼性の高い位置情報の生成・記録方式、そしてそれらのソフトウェア・ハードウェアの開発、社会実装における評価・検証を行う。

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/B5Gsokushin/B5G_03901.html）
電話 042－327－6011

将来の方向性

次世代の物流に不可欠なセキュリティ基盤技術を確立し、Beyond 5G推進戦略が目指すSociety 5.0の実現に寄与する。

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　不正プログラム対策技術

テーマ名　Web媒介型攻撃対策技術

開発年度　平成30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

サイバー攻撃は、多様化・巧妙化を続け、Webサイトを閲覧するだけでマルウェアに感染するWeb媒介型攻撃による被害が続いている。Web媒介型攻撃は、特定のWebサイトを閲覧したユーザーに対してのみ攻撃が行われるため、受動的なサイバー攻撃観測網では、正確な攻撃の実態把握が困難である。そこで、このプロジェクトでは、ユーザー参加型の攻撃観測網を構築し、集まったデータをプロジェクト参画組織と共同分析することによって、攻撃の実態解明や攻撃対策の展開を目指す。

研究開発状況（概要）

これまでにPC版、モバイル版の２つのデバイス向けのセンサーエージェントを開発公開している。ローカルネットワークスキャン機能を新たに開発し取得可能データを拡張した。その他センサーのさらなる高度化、ユーザー増、定着率の向上を目的とした機能の拡張を行った。収集したデータをプロジェクト参画組織と共同分析し、対策技術の拡張とユーザーへのフィードバックを推進した。

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ネクサス 042-327-5246

将来の方向性

継続してセンサーエージェントの高度化を行うと共に、ユーザー増、定着率向上を通じて共同分析可能なデータ量を増加させ、収集したデータの共同分析により安全・安心な情報通信基盤の実現を目指す。

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、高いセキュリティと効率性（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、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暗号化した状態で検索や計算を行う秘密計算技術（秘密計算に関し、秘匿データベースシステムについて企業との連携で実用化事例あり）、自分が誰かを明かさないまま正規のユーザであることなどを証明できる匿名認証技術等の開発を継続的に行っている。

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。

対象技術　脆弱性探査技術、ペネトレーション技術

テーマ名　サイバー空間の状況把握・防御技術の向上及び共通基盤の整備

開発年度　令和６年度～令和１１年度（予定）

実施主体　一般社団法人サイバーリサーチコンソーシアム（国立研究開発法人 新エネルギー・産業技術総合開発機構が実施する委託研究の委託先）

法人番号　2021005012927

背景、目的

高度かつ未知の攻撃にも対処可能な攻撃の早期発見技術、攻撃者からより多くの情報を獲得するための技術などのサイバー空間の情報を収集・調査する状況把握力の向上に資する技術を開発し、社会実装につなげる。

AIを活用した脆弱性の検知・評価技術、耐量子計算機暗号の実装技術、ペネトレーションテストなどの検証手法自動化技術などの防御力向上に資する技術を開発し、社会実装につなげる。

情報に関する共有基盤の最適化と構築を行う。また、高度サイバー人材の評価・管理に関する技術を開発し展開する。

研究開発状況（概要）

以下の研究開発を実施中。

①サイバー空間の情報を収集・調査する状況把握力向上

・ アーティファクト分析技術／攻撃者からより多くの情報を獲得するための技術／高度かつ未知の攻撃にも対処可能な攻撃の早期発見技術

②サイバー攻撃から機器やシステムを守る防衛力向上

・ AIを活用した脆弱性探査技術／AI等を活用した防御能力の評価・向上技術／AIを活用したOTペネトレーションフレームワーク技術

・ 耐量子計算機暗号技術／耐タンパー性向上技術

③共通基盤の整備

・ 情報の効果的な連携に関わる技術

・ 高度サイバー人材の評価・管理に関する技術

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 新エネルギー・産業技術総合開発機構 半導体・情報インフラ部
E-mail：kpro_cyber[*]nedo.go.jp
※[*]を@に変えて使用

将来の方向性

サイバー空間の情報を収集・調査する状況把握力、サイバー攻撃から機器やシステムを守る防御力の向上、ならびにそれら能力・技術の評価技術と評価環境の開発・展開を目指す。

（別添２）

ア　大学

企業・大学名	学校法人名古屋電気学園愛知工業大学
代表者名	後藤 泰之
所在地	470-0392 愛知県豊田市八草町八千草1247
窓口部署名	総務課
電話番号	0565-48-8121
関連部門名	情報科学部 情報科学科 モバイルコンピューティング研究室
ホームページのURL	https://www.ait.ac.jp/
研究説明のURL	https://researchmap.jp/katsuhiro.naito/published_papers
対象技術	研究開発状況
研究開発名称： CYPHONIC 研究開発国： 日本 研究開発時期： 2018年4月1日～	管理クラウド機能と端末機能の実装は概念実証は終えておりマネージメント機能の強化及びクラウド側のDDoS対策などを検討中

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	

企業・大学名	公立大学法人大阪
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報学研究科
ホームページのURL	
研究説明のURL	なし
対象技術	研究開発状況
研究開発名称： ネットワークトラフィック及びログ解析に基づく異常検知 研究開発国： 日本 研究開発時期： 2006年4月1日～2024年	基礎研究を継続しており、研究成果は国内の学会等で継続的に発表している。

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	公立大学法人北九州市立大学
代表者名	理事長　津田　純嗣
所在地	802-8577 福岡県北九州市小倉南区北方四丁目２番１号
窓口部署名	企画管理課　企画・研究支援係
電話番号	093-695-3367
関連部門名	情報システム工学科　山崎恭研究室
ホームページのURL	https://www.kitakyu-u.ac.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 高度生体認証システム 研究開発国： 日本 研究開発時期： 2020年4月1日～2025年3月31日	科学研究費助成事業の研究課題において，携帯端末を対象とした安全性および利便性の高い生体認証システム（高度生体認証システム）を実現するための要素技術を開発中.

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	

企業・大学名	国立大学法人東海国立大学機構岐阜大学
代表者名	松尾　清一
所在地	501-1193 岐阜市柳戸１－１
窓口部署名	研究推進部研究推進課
電話番号	058-293-3140
ホームページのURL	https://ari.gifu-u.ac.jp/
対象技術	技術の概要・特徴など
製品名： Microsoft AZURE 開発元(メーカー名等)： Microsoft 開発国： アメリカ 価格： https://azure.microsoft.com/ja-jp/pricing/details/cognitive-services/openai-service/?msockid=2c44f817717566f51281eb5a70fe6745 発売時期： 2010年1月1日 出荷数： 増加中 https://www.nikkei.com/article/DGXZQOGN27EC70X20C21A7000000/?msockid=2c44f817717566f51281eb5a70fe6745	https://azure.microsoft.com/ja-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	国立大学法人東海国立大学機構岐阜大学
代表者名	松尾　清一
所在地	501-1193 岐阜市柳戸１－１
窓口部署名	研究推進部研究推進課
電話番号	058-293-3140
関連部門名	研究推進部
ホームページのURL	https://ari.gifu-u.ac.jp/
研究説明のURL	特になし
対象技術	研究開発状況
研究開発名称： オープンイノベーションサーバー 研究開発国： 日本 研究開発時期： 2022年9月1日～2023年3月20日	研究データのオリジナル性を担保するために、ブロックチェーンの仕組みを使っています。

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	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	研究開発状況
研究開発名称： イントラネットにおけるデバイスの柔軟なアクセス制御に関する研究 研究開発国： 日本 研究開発時期： 2022年4月～	要素技術としてLinuxカーネルに搭載されているeBPF（extended Berkeley Packet Filter）に着目している．eBPFは，デバイスの様々な情報を精密に監視する手段として近年注目されている．現在は，eBPFを活用し，通信情報を構成するパケットと、パケットを送受信したアプリケーションを関連付けるシステムの実現性と有効性を検証している．今後，パケットに関連付けられたアプリケーション情報を利用した，柔軟かつ細粒度なアクセス制御システムの開発を進める．

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	東京情報大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	総合情報学部 共創ラボ（ネットワーク・セキュリティ Lab）
ホームページのURL	https://www.tuis.ac.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 情報システムに対する攻撃・不正アクセスの予測・検知・防御・分析・可視化に関する基盤技術の確立 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	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	情報学研究科 情報システム学専攻 嶋田研究室
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	研究開発状況
研究開発名称： （特にプロジェクト名は無い） 研究開発国： 日本 研究開発時期：	以下のような研究を過去数年の間に実施している。継続的に研究開発を続けているため、研究開発期間は特に記さない。 - 悪性通信の解析/検知 - HTTP(S)通信を使うC&C通信の検出 - NFA型シグネチャ検知のFPGAによるハードウェア化 - FPGAを利用したペイロードの周波数領域特徴量抽出とホストPCでの機械学習系検知 - マルウェアの検知/分類 - マルウェアバイナリのCFG特徴のGINによる圧縮を利用した分類 - カスタム損失関数を導入したGBDTによるマルウェア検知精度向上 - 潜在表現の時系列差分を用いた亜種マルウェア検知精度向上 - セキュアなネットワーク運用 - 攻撃の進捗と業務継続性を両立するネットワーク遮断 - OS間のIPv6実装状態の差を悪用する攻撃と検証 - バックボーン遅延ヒストグラムからの無線LAN Rogue AP(偽AP)検知 - 自動リンク処理などにおける国際化ドメイン名などUTF文字処理上のセキュリティ問題 - Physically Unclonable Functionを利用したIoT向けプロトコルの多要素認証化 - セキュリティナレッジの構築 - SNSや議論系Webサイトから脆弱性情報の収集とランク分け - SNSの脆弱性話題からのWeb Application Firewallルール生成 - ハニーポットとIDS - IoT向け通信プロトコルのためのハニーポットとその観測結果 - 標的型攻撃対策 - ログ統合によるサイバー攻撃推定手法 - ユーザの信用度を考慮したテレワーク通信へのアクセス制御手法 - 通信遮断による標的型攻撃対応のための影響範囲VR可視化システム - 機械学習/深層学習応用システムへの攻撃 - 研究用IDS作成学習データセットに対する偽学習データ付与 - 勾配情報変化量を利用したSVMベースのマルウェア検知を標的にする中毒攻撃データの検知 - 悪性URLクエリを検知する機械学習システムに対する細工されたURLクエリ学習による中毒攻撃とその対策

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	日本文理大学
代表者名	学長　橋本　堅次郎
所在地	870-0397 大分県大分市一木1727
窓口部署名	大学総務・経理担当
電話番号	097-524-2700
関連部門名	日本文理大学・工学部・情報メディア学科
ホームページのURL	https://www.nbu.ac.jp/
研究説明のURL	www.nbu.ac.jp/~fukushima/fukushima.html
対象技術	研究開発状況
研究開発名称： 非記号情報による環境状況推定 研究開発国： 日本 研究開発時期： 2024年4月1日～2025年3月31日	企業との共同研究として進行している

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	研究開発状況
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	研究開発状況
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	研究開発状況
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	研究開発状況
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	学校法人福岡大学
代表者名	
所在地	
窓口部署名	
電話番号	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： 　パスワード共有サービス 　PASSPATH 開発元(メーカー名等)： 　福岡大学情報基盤センター中 　國研究室 開発国： 　日本 価格： 　現在は無料 発売時期： 出荷数：	現在話題になっているPPAP（パスワードの後送問題）を解決するソリューションである。 サービスを提供しているサイトのURLは下記のとおり。 https://passpath.net/

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	研究開発状況
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～2025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、近々、多くの被験者を用いて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について協議しており、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	公立大学法人前橋工科大学
代表者名	理事長　福田尚久
所在地	371-0816 群馬県前橋市上佐鳥町460番地1
窓口部署名	学務課　地域貢献・研究支援係
電話番号	027-265-7361
関連部門名	-
ホームページのURL	https://www.maebashi-it.ac.jp/
研究説明のURL	https://kaken.nii.ac.jp/ja/grant/KAKENHI-PROJECT-23K11104/
対象技術	研究開発状況
研究開発名称： 高速処理と柔軟なポリシー記述を可能にする次世代フィルタの開発 研究開発国： 日本 研究開発時期： 2023年4月1日～2026年3月31日	パケット分類アルゴリズムの開発状況について、現在、領域分割アルゴリズムと連分割トライアルゴリズムとの融合に関する実装を完了している段階である。提案アルゴリズムについて、理論的な評価では、非常に高速な分類処理速度を達成している一方で、ランダムに抽出したデータで構成される疑似ネットワーク環境において要求メモリ量が莫大であり、実用上問題がある段階である。今後は、実際のネットワーク環境を模倣した作成されたデータを使用して、提案アルゴリズムの調整を進めていく予定である。

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	明星大学 情報学部
代表者名	
所在地	191-8506 東京都日野市程久保2-1-1
窓口部署名	明星大学　情報学部支援センター
電話番号	
関連部門名	情報学部 情報学科 丸山研究室
ホームページのURL	（明星大学情報学部） https://www.is.meisei-u.ac.jp/ （明星大学） https://www.meisei-u.ac.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 可読文字列と画像化技術を併用したマルウェア判別手法 研究開発国： 日本 研究開発時期： 2024年6月～	マルウェア解析における表層解析は，補助的な役割に限定して利用されてきた．ファイルの可読文字列やバイナリデータなどを調査する表層解析は，実際にマルウェアを動かしているわけではない．そのため，解析にかかる時間が短く，簡単に行うことができる一方，得られる情報が少ない．しかし，自然言語処理技術や深層学習などの発達により，表層解析は再評価された．現在では，可読文字列やバイナリデータなど表層解析から得られる情報のみを利用して，マルウェアの検知や分類を行う手法が提案されている． 本研究では，可読文字列と画像化技術の併用によるマルウェア検知率及び判別率の向上を目的とする．

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	明星大学 情報学部
代表者名	
所在地	191-8506 東京都日野市程久保2-1-1
窓口部署名	明星大学　情報学部支援センター
電話番号	
関連部門名	情報学部 情報学科 丸山研究室
ホームページのURL	（明星大学情報学部） https://www.is.meisei-u.ac.jp/ （明星大学） https://www.meisei-u.ac.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 覗き見耐性を持つジャイロと音を用いた認証手法 研究開発国： 日本 研究開発時期： 2024年6月～	スマートフォンのロック解除において覗き見攻撃を防ぐために振動やジェスチャーを用いた認証がこれまで提案されてきているが，覗き見されてしまい，パスワードが盗まれてしまう可能性が残っている．また，画面の視覚情報を用いない認証方式については，検討がされていない現状がある． 本研究ではスマートフォンに内蔵されているジャイロセンサと，常時装着することが増えているヒアラブルデバイス（完全ワイヤレスイヤホン）からの音を用いた，画面の視覚情報を用いない新たな認証手法について検討する．

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	明星大学 情報学部
代表者名	
所在地	191-8506 東京都日野市程久保2-1-1
窓口部署名	明星大学　情報学部支援センター
電話番号	
関連部門名	情報学部　情報学科　小暮研究室
ホームページのURL	（明星大学情報学部） https://www.is.meisei-u.ac.jp/ （明星大学） https://www.meisei-u.ac.jp/
研究説明のURL	https://www.iag.meisei-u.ac.jp/meuhp/KgApp?resId=S001191&_gl=1*14z5mzy*_ga*MTEzODYxMzY3NS4xNjUzNDQ5OTcx*_ga_FWWP82PEWW*MTcyNjYOMTAxMS41NC4xLjE3MjY2NDEwNjMuMC4wLjA.*_ga_EB871D7KTK*MTcyNjYOMTAxMS41NC4xLjE3MjY2NDEwNjMuMC4wLjA.*_ga_9XN59YCSYK*MTcyNjYOMTAxMS41MS4xLjE3MjY2NDEwNjMuMC4wLjA.
対象技術	研究開発状況
研究開発名称： 暗号技術・認証技術 研究開発国： 日本 研究開発時期： 2021年7月1日～2027年3月31日	誰でもインターネットにアクセスすることのできる現代社会においては、デジタルデータで表現される情報を安全に守る必要があります。デジタルデータの秘匿に用いられる暗号技術の安全性を、数学を用いた解読計算量の観点から保証する研究を行っています。世界中で通用する仮想通貨を初めて実現したブロックチェーン等、コンピューターを通じて数学と社会とをつなぐアプリケーションの研究開発も行っています。

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	国立大学法人 横浜国立大学
代表者名	学長　梅原　出
所在地	240-8501 横浜市保土ヶ谷区常盤台79-1
窓口部署名	研究・学術情報部　情報企画課　情報企画係
電話番号	045-339-4472
関連部門名	先端科学高等研究院　情報・物理セキュリティ研究ユニット
ホームページのURL	https://www.ynu.ac.jp/
研究説明のURL	https://sec.ynu.codes/iot/ https://sec.ynu.codes/dos http://yoshioka.ynu.ac.jp/research.html https://ipsr.ynu.ac.jp/outcome.html
対象技術	研究開発状況
研究開発名称： セキュリティインテリジェンス提供サービス 研究開発国： 日本 研究開発時期： 2015年1月1日～2025年12月31日	サイバー攻撃やその原因となっている脅威アクターの動向をインターネット上のクロールやハニーポットにより観測し、情報を蓄積しており、そのデータを外部に提供する形でのサービスを提供する可能性がある。ハニーポットによる観測は９年間の研究開発を行っており、脅威アクタ分析については2022年度から開発を実施している。

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　琉球大学
代表者名	西田　睦
所在地	903-0213 沖縄県中頭郡西原町字千原１
窓口部署名	工学部総務係
電話番号	098-895-8589
関連部門名	工学部
ホームページのURL	https://www.tec.u-ryukyu.ac.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： USBメモリ紛失時の情報漏えい検知技術に関する研究開発 研究開発国： 日本 研究開発時期： 2024年4月1日～	USBメモリを紛失して拾得された際に、デバイス内の情報にアクセスされたことを検知する技術を研究している。 現在その有効性やユースシーンについて情報収集、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	和歌山大学
代表者名	
所在地	640-8510 和歌山県和歌山市栄谷930
窓口部署名	
電話番号	
関連部門名	情報セキュリティ
ホームページのURL	https://www.wakayama-u.ac.jp/
研究説明のURL	（なし）
対象技術	研究開発状況
研究開発名称： 情報危機管理教育サービス 研究開発国： 日本 研究開発時期： 2024年4月1日～2026年3月31日	当方は、「情報危機管理コンテスト」を19年間実施しており、その運用を担当している。当該コンテストは、情報セキュリティに関するインシデントを当方が発生させ、コンテスト参加側がインシデント対応し、その技量を競うものである。 上記コンテスト運用は、一種の教育システムとして設計しており、和歌山大学内外での情報セキュリティ実践演習としても活用している。しかし、同様にリソースの限度によって展開が困難となっており、これを解決するための研究開発としている。 現在、クラウド化について、いくつかのインシデント・シナリオを実装しており、現在は生成AIによる人的資源のリプレースを設計している。今後は、100人を受け入れるためのシステム設計、インタフェースの開発を実施する予定である。

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	

イ　企業

企業・大学名	株式会社アイ・エス・ビー
代表者名	代表取締役社長　岩尾一史
所在地	141-0032 東京都品川区大崎5-1-11
窓口部署名	総務部
電話番号	03-3490-1761
ホームページのURL	https://www.isb.co.jp
対象技術	技術の概要・特徴など
製品名： Fit SDM 開発元（メーカー名等）： (株)アイ･エスビー 開発国： 価格： 150円～800円/月額 発売時期： 出荷数： 	MDMです　クライドサービスとして提供

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	株式会社ソリトンシステムズ
代表者名	鎌田 理
所在地	160-0022 東京都新宿区新宿２－４－３
窓口部署名	ITセキュリティ事業部
電話番号	03-5360-3811
ホームページのURL	https://www.soliton.co.jp/
対象技術	技術の概要・特徴など
製品名： Soliton OneGate 開発元(メーカー名等)： 株式会社ソリトンシステムズ 開発国： 日本 価格： PKIプラン 100円/月、Basicプラン 300円/月、Standardプラン 600円/月など。詳細はお問い合わせください。 発売時期： 2019年12月2日 出荷数： 非開示	Soliton OneGateは、デジタル証明書をはじめとする多彩な多要素認証（MFA）とシングルサインオン（SSO）でクラウドに点在する組織の情報資産を不正アクセスから守る、多要素認証サービスです。 クラウドからデータを持ち出さずに活用することができるセキュアブラウザ機能を使った「データ保護」（情報漏えい対策）や、セキュアな無線LAN認証やVPN/SASE認証の強化、Windowsサインインの認証強化にも対応し、セキュリティ強化で組織のDX推進を支援します。 ※政府情報システムのためのセキュリティ評価制度（ISMAP）に登録済み。

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	株式会社ソリトンシステムズ
代表者名	鎌田 理
所在地	160-0022 東京都新宿区新宿２－４－３
窓口部署名	ITセキュリティ事業部
電話番号	03-5360-3811
ホームページのURL	https://www.soliton.co.jp/
対象技術	技術の概要・特徴など
製品名： NetAttest EPS 開発元(メーカー名等)： 株式会社ソリトンシステムズ 開発国： 日本 価格： NetAttest EPS(EPS-SX15A-A モデル) 定価23万円～、物理・仮想アプライアンスで複数のラインナップがあり、ご利用機能に応じたライセンスと保守費用が必要です。詳細はお問い合わせください。 発売時期： 2002年 出荷数： 累計33,000台以上	NetAttest EPSは、オールインワン認証アプライアンスです。ネットワーク機器と連携して強固な認証環境を実現し、悪意ある攻撃者の不正侵入をシャットアウトします。 デジタル証明書を利用したネットワーク認証に必要となる機能を搭載し、正しい端末・正しいユーザーのみネットワークに接続できる安全な環境を実現することができます。無線LANセキュリティとして求められているIEEE802.1XのEAP-TLS認証、VPNの多要素認証（MFA）を実現する認証サーバーとして、多くの実績があります。

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	