令和８年３月 12 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７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７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

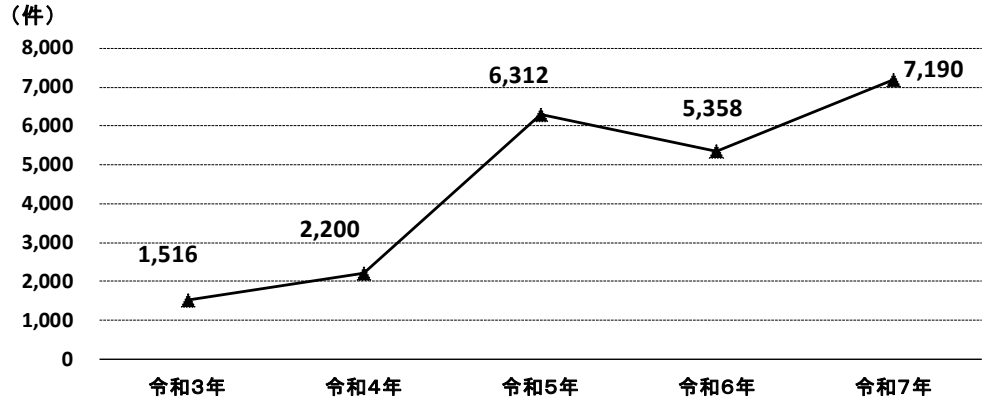
令和７年に都道府県警察から警察庁に報告がなされた不正アクセス行為の認知・検挙状況等は次のとおりである。

１　不正アクセス行為の認知状況

(1)　認知件数

令和７年における不正アクセス行為の認知件数[注1]は 7,190 件であり、前年（令和６年）と比べ、1,832 件（約 34.2%）増加した。

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７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（4,747 件）、次いで「証券会社のインターネット取引サービスでの不正取引等」（1,484 件）、「インターネットショッピングでの不正購入」（228 件）の順となっている。

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。

図１－２　令和７年における不正アクセス後の行為別認知件数

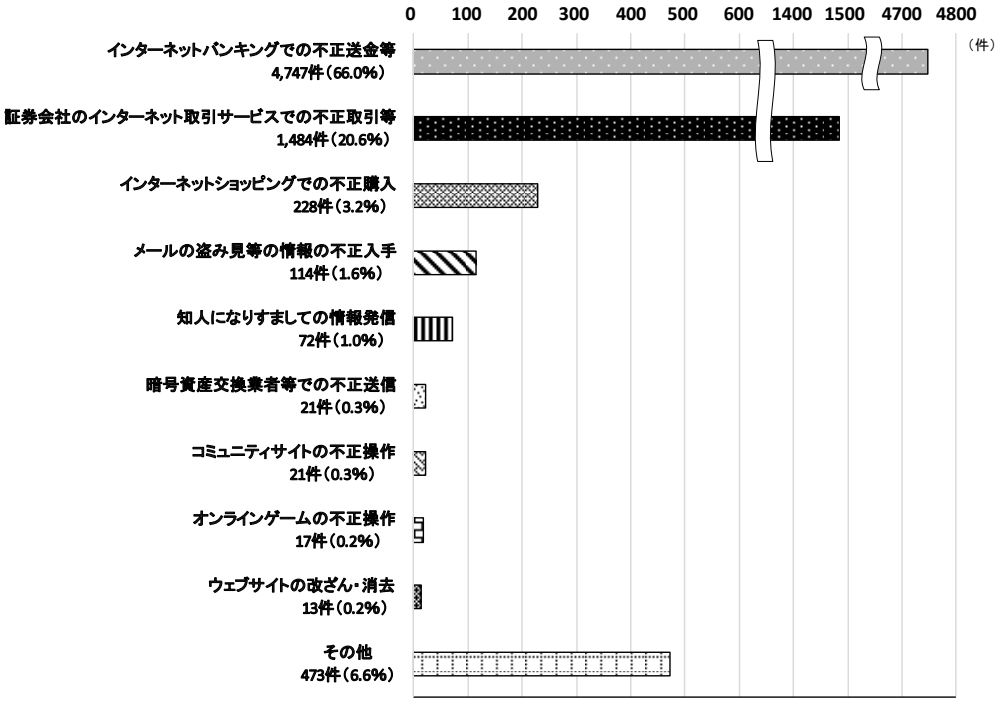


表１－１　不正アクセス後の行為別認知件数（過去５年）

区分＼年次	令和3年	令和4年	令和5年	令和6年	令和7年
インターネットバンキングでの不正送金等	693	1,096	5,598	4,342	4,747
証券会社のインターネット取引サービスでの不正取引等	0	0	0	2	1,484
インターネットショッピングでの不正購入	349	227	93	180	228
メールの盗み見等の情報の不正入手	175	215	204	192	114
知人になりすましての情報発信	71	50	33	69	72
暗号資産交換業者等での不正送信	20	32	14	21	21
コミュニティサイトの不正操作	49	34	65	42	21
オンラインゲームの不正操作	16	29	18	21	17
ウェブサイトの改ざん・消去	8	17	8	9	13
その他	135	500	279	480	473
計	1,516	2,200	6,312	5,358	7,190

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７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431件・248人であり、前年（令和６年）と比べ、132件減少し、検挙人員は11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407件・236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６件・４人、「識別符号提供（助長）行為[注3]」が８件・８人、「識別符号保管行為[注4]」が８件・８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3年	令和4年	令和5年	令和6年	令和7年
不正アクセス行為	検挙件数	408	491	487	533	407
	検挙事件数 注6	189	223	216	228	223
	検挙人員	227	243	248	252	236
識別符号取得行為	検挙件数	4	8	11	3	6
	検挙事件数	2	5	4	2	4
	検挙人員	2	5	8	2	4
識別符号提供(助長)行為	検挙件数	9	5	13	11	8
	検挙事件数	8	5	6	4	8
	検挙人員	8	5	10	4	8
識別符号保管行為	検挙件数	7	16	7	14	8
	検挙事件数	6	8	6	9	8
	検挙人員	6	8	6	9	8
識別符号不正要求行為	検挙件数	1	2	3	2	2
	検挙事件数	1	2	2	2	2
	検挙人員	1	2	2	2	2
計	検挙件数	429	522	521	563	431
	検挙事件数	195 (重複11)	237 (重複6)	221 (重複13)	232 (重複13)	235 (重複10)
	検挙人員	235 (重複9)	257 (重複6)	259 (重複15)	259 (重複10)	248 (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７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 399 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3年	令和4年	令和5年	令和6年	令和7年
識別符号窃用型	検挙件数	398	482	475	511	399
	検挙事件数	182	215	207	210	216
セキュリティ・ホール攻撃型 注8	検挙件数	10	9	12	22	8
	検挙事件数	8	8	10	18	8
計	検挙件数	408	491	487	533	407
	検挙事件数	189 （重複1）	223	216 （重複1）	228	223 （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。

注8　アクセス制御機能のプログラムの瑕疵（かし）、アクセス管理者の設定上のミス等のコンピュータ・システムにおける安全上の不備を突く行為いう。

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７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（91 人）、次いで「14～19 歳」（81 人）、「30～39 歳」（41 人）の順となっている[注9]。

なお、令和７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 10 歳[注10]、最年長の者は 65 歳であった。

図３－１　令和７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

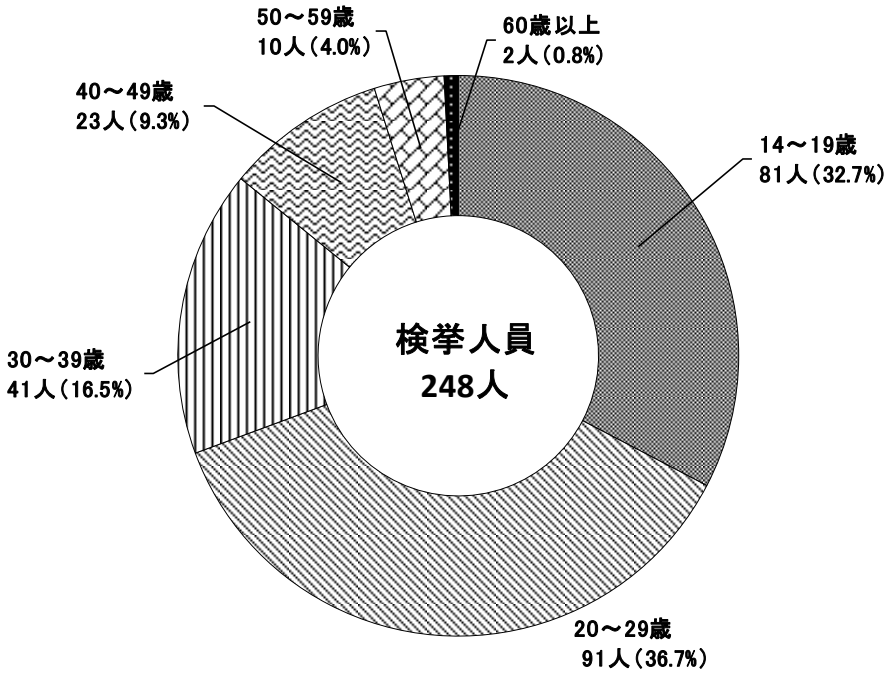


表３－１　年齢別被疑者数の推移（過去５年）

区分＼年次	令和3年	令和4年	令和5年	令和6年	令和7年
14～19歳	60	68	73	72	81
20～29歳	87	104	103	105	91
30～39歳	43	55	53	42	41
40～49歳	30	15	21	18	23
50～59歳	11	14	8	17	10
60歳以上	4	1	1	5	2
計	235	257	259	259	248

注9　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10　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７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（399 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（84 件）、次いで「フィッシングサイトから入手」（77 件）の順となっており、前年（令和６年）と比べ、前者は 90 件減少、後者は 36 件増加となっている。

図３－２　令和７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

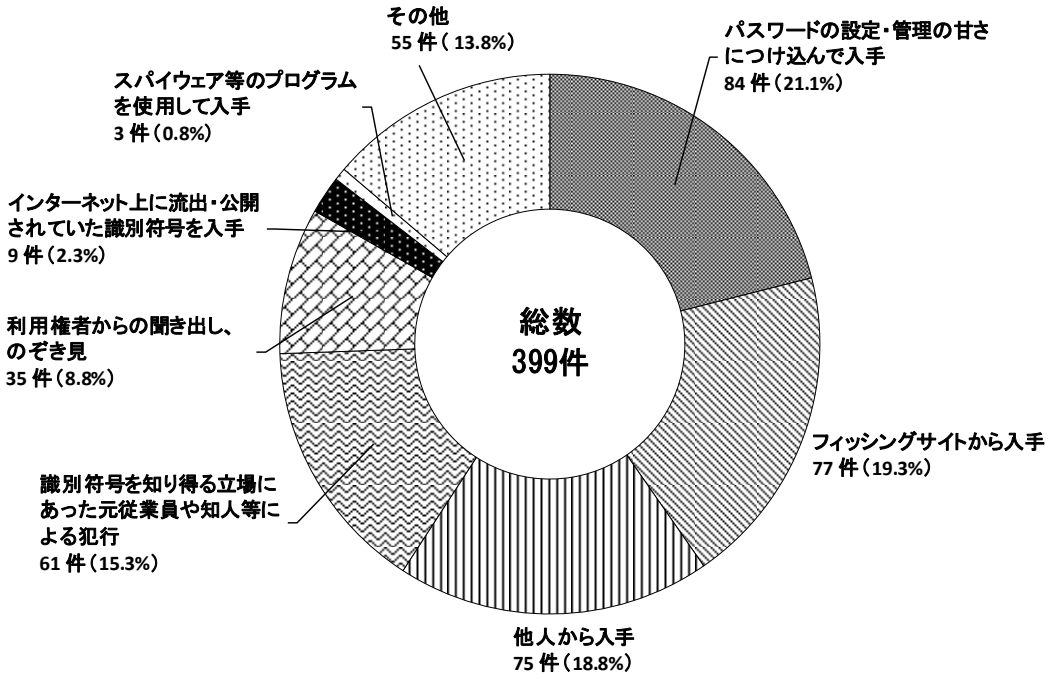


表３－２　不正アクセス行為の手口別検挙件数（過去５年）

区分＼年次		令和3年	令和4年	令和5年	令和6年	令和7年
識別符号窃用型		398	482	475	511	399
	パスワードの設定・管理の甘さにつけ込んで入手	153	230	203	174	84
	フィッシングサイトから入手	70	14	10	41	77
	他人から入手	34	27	36	67	75
	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	51	41	68	107	61
	利用権者からの聞き出し、のぞき見	36	38	40	51	35
	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	2	9	2	11	9
	スパイウェア[注11]等のプログラムを使用して入手	0	0	2	0	3
	その他	52	123	114	60	55
セキュリティ・ホール攻撃型		10	9	12	22	8

注11　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７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（399 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（122 件）、次いで「コミュニティサイト」（92 件）の順となっており、前年（令和６年）と比べ、前者は 99 件減少、後者は 16 件減少となっている。

図３－３　令和７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

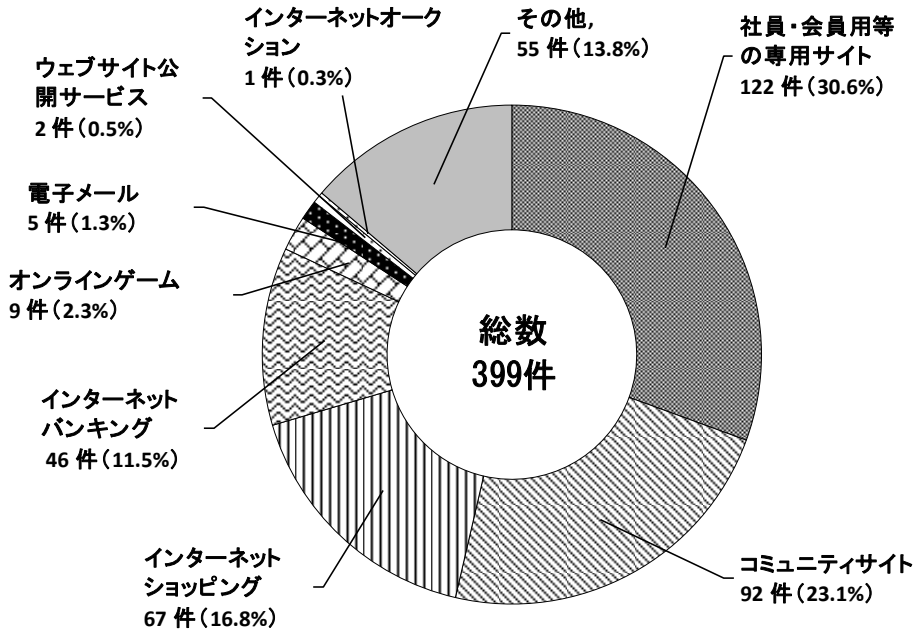


表３－３　不正アクセス行為（識別符号窃用型）により不正に利用されたサービス別検挙件数（過去５年）

区分＼年次	令和3年	令和4年	令和5年	令和6年	令和7年
社員・会員用等の専用サイト	75	104	82	221	122
コミュニティサイト	135	206	225	108	92
インターネットショッピング	38	26	35	69	67
インターネットバンキング	96	17	29	40	46
オンラインゲーム	9	27	9	11	9
電子メール	14	14	3	10	5
ウェブサイト公開サービス	4	8	0	0	2
インターネットオークション	0	0	0	0	1
インターネット接続サービス	0	1	0	0	0
その他	27	79	92	52	55
計	398	482	475	511	399

４　令和７年の主な検挙事例

(1)　ＳＮＳで結びついた中高生の少年３人（14 歳から 16 歳）は、不正に取得したｅＳＩＭ[注12]を販売して利益を得ようと考え、令和６年５月から同年８月までの間に、それぞれ、不正に取得した他人のＩＤ・パスワードを使い、電気通信事業者が管理するサーバコンピュータに不正アクセスした上で、通信契約に係る不実の電磁的記録を作成し、ｅＳＩＭを不正に取得した。令和７年１月から同年２月にかけて、同少年ら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。

(2)　上記(1)の手口を模倣し、不正に取得したｅＳＩＭを販売して利益を得ようと考え、令和６年４月、無職の少年（16 歳）と高校生の少年（16 歳）が、模倣した手口によりｅＳＩＭを不正に取得したことを受け、令和７年３月、同少年ら２人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。

(3)　職業不詳の男（29 歳）らが、令和６年６月、生成ＡＩを一部悪用するなどして構築した大手ＥＣサイトを模したフィッシングサイトを公開した。令和７年６月、同男らを不正アクセス禁止法違反（識別符号不正要求行為）で検挙した。

(4)　会社経営の男（38 歳）らが、令和７年３月、氏名不詳者らと共謀の上、証券会社が管理する認証サーバコンピュータに不正にアクセスし、他人名義口座で上場されている特定の株式の売買を行うなどして不正に株価を上昇させ利益を得たことを受け、同男らを不正アクセス禁止法違反（不正アクセス行為）及び金融商品取引法違反で検挙した。

(5)　無職の少年（17 歳）が、令和６年 10 月から同年 11 月までの間に、電子決済サービスを模した自作のフィッシングサイトのＵＲＬをＳＮＳで送信し、利用権者に銀行の口座情報を入力させて同情報を窃取し、当該情報を用いて銀行口座に不正アクセスした上、別人名義の口座に不正送金するなどしたことを受け、同少年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。

注12　Embedded Subscriber Identity Module。スマートフォン等の端末内にＳＩＭが内蔵されている本体一体型のＳＩＭのこと。

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13]や二経路認証[注14]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

注13　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14　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

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)　ウェブシステムやＶＰＮ機器のぜい弱性を悪用した攻撃への対策

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、フィッシングに耐性のある認証技術（例：パスキー[注15]）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、自社のドメインになりすましたフィッシングメールの悪用を防止する観点で送信ドメイン認証技術（ＤＭＡＲＣ[注16]、ＳＰＦ[注17]、ＤＫＩＭ[注18]）を計画的に導入し、ＤＭＡＲＣの導入に当たっては、受信側に対してなりすましメールの受信拒否を要求するポリシーでの運用を行う。

注15　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16　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。送信側は、受信側が認証に失敗したメールの取扱いを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、といったポリシーを受信側に伝えることができるようになる。

注17　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18　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７年（令和７年１月１日から令和７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19]の届出件数は 109 件（令和６年：166 件）であった[注20]。令和７年は令和６年と比べて、57 件（約 34.3%）減少した。

この届出がなされた中には、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、ＩＰＡが把握できた範囲では、届出で主に見受けられたものとして、ＶＰＮ装置のぜい弱性の悪用や認証情報の不正利用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。）のぜい弱性を悪用した攻撃による改ざん被害、インターネットサービス（Microsoft 365 等）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、一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。

なお、各項目の主な内容については項目ごとに上位３分類を記載している。

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 237 件(令和６年:407 件)であった（一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。）。

(1)　侵入行為

侵入行為に係る攻撃等に分類した件数は 167 件（令和６年：316 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。

０件であった（本期間中の届出には含まれていなかった。）。

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、ソフトウェアのバグ等のいわゆるぜい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。

61 件あり、その主な内容を次に示す。

【主な内容】

パスワード推測（パスワードリスト攻撃等）：31 件

ぜい弱性を悪用した攻撃：21 件

システムの設定不備を悪用した攻撃：９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。

注19　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20　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。

106 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：65 件

不正プログラムの埋め込み：34 件

資源利用（ＣＰＵ等のリソース不正使用）：５件

(2) 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能な状態にさせ、又はサービスの質を低下させる攻撃で、４件（令和６年：８件）であった。

(3) 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。66 件（令和６年：83 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：26 件

不審メール（スパムメール、フィッシングメール、ＳＭＳ等）：18 件

他サイト侵入のための踏み台：10 件

２ 原因別分類

109 件の届出のうち、実際に被害に遭った 85 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 89 件（令和６年：141 件）であった（一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、届出がなされる中には「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】

ＩＤ・パスワード管理の不備：30 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：18 件

原因不明：15 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。）：７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。

一つの届出において、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】

クライアント：28 件

ウェブサーバ：27 件

ファイルサーバ：19 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 195 件（令和６年：328 件）であった（一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：44 件

ファイルの書換え：34 件

不正プログラムの埋め込み：32 件

５　対策情報

令和７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みられた。これらを含む、原因別で分類した89件の原因を割合で示すと「ＩＤ・パスワード管理の不備」が約33.7%（30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」が約20.2%（18件）であり、この二つの項目で約53.9%（48件）と大きな割合を占めている。また、「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7.9%（７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ぜい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ぜい弱性診断の実施
- 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、着実にシステムのぜい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。ぜい弱性はシステムの導入時のみでなく、運用開始後にも発生するものであるため、導入時の入念な確認と継続的なぜい弱性対応は必要であることに留意されたい。また、前述したように、侵入の事前調査行為に関する届出がなかったことや、不正アクセスの原因を「原因不明」とする届出も多いことから、ログ取得や保管の方法、取得する期間を見直すなどのほか、自組織だけではなく外部機関に対応を依頼するなどして、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
- パスワードの使い回しをしない
- 多要素認証等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。

加えて、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

情報セキュリティ対策に関しては、次を参照することを勧める。
・「中小企業の情報セキュリティ対策ガイドライン」
https://www.ipa.go.jp/security/guide/sme/about.html
ウェブサイトのぜい弱性を悪用した攻撃等への対策に関しては、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)」 ※ぜい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への対策として、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

○　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及び件数

令和７年にＪＰＣＥＲＴ／ＣＣに報告（調整対応依頼）のあった不正アクセス関連行為[注21] 係わる報告件数[注22]は 68,853 件であった。この報告を元にしたインシデント件数[注23]は 38,345 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とおりである。

(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 1,417 件の報告があった。

[1/1-3/31: 256 件、4/1-6/30: 240 件、7/1-9/30: 452 件、10/1-12/31: 469 件]

(2)　Ｗｅｂサイト改ざん

攻撃者又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 750 件の報告があった。

[1/1-3/31: 95 件、4/1-6/30: 231 件、7/1-9/30: 319 件、10/1-12/31: 105 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 127 件の報告があった。

[1/1-3/31: 23 件、4/1-6/30: 28 件、7/1-9/30: 32 件、10/1-12/31: 44 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 16 件の報告があった。

[1/1-3/31: ６件、4/1-6/30: ２件、7/1-9/30: ２件、10/1-12/31: ６件]

(5)　Ｗｅｂ偽装事案（フィッシング）

Ｗｅｂのフォーム等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 34,085 件の報告があった。

[1/1-3/31: 5,267 件、4/1-6/30: 7,358 件、7/1-9/30: 9,063 件、
10/1-12/31: 12,397 件]

注21　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（又は偶発的）に発生する全ての事象が対象になる。

注22　ここに挙げた件数は、ＪＰＣＥＲＴ／ＣＣ が受け付けた報告の件数である。当該件数を基に実際のアタックの発生件数や、被害件数を類推することはできない。また、類型ごとの実際の発生比率を示すものでもない。一定以上の期間にわた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的に対応しない。報告元には、国内外のサイトが含まれる。

注23　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、一つのインシデントに関して複数件の報告が寄せられた場合は、１件のインシデントとして扱う。

(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、業種等を標的として、マルウェア感染や情報の窃取等を試みる攻撃について 12 件の報告があった。

[1/1-3/31: １件、4/1-6/30: ５件、7/1-9/30: ３件、10/1-12/31: ３件]

(8) その他

コンピュータウイルス、ＳＰＡＭメールの受信等について 1,938 件の報告があった。

[1/1-3/31: 433 件、4/1-6/30: 484 件、7/1-9/30: 508 件、10/1-12/31: 513 件]

２ 防御に関する啓発及び対策措置の普及

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等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
2025 年１月	Ivanti Connect Secure等におけるぜい弱性（CVE-2025-0282）に関する注意喚起（公開）
	Fortinet 製 FortiOS 及び FortiProxy における認証回避のぜい弱性（CVE-2024-55591）に関する注意喚起（公開）
	2025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）
2025 年２月	2025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）
2025 年３月	Adobe Acrobat 及び Reader のぜい弱性（APSB25-14）に関する注意喚起（公開）
	2025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）
	a-blog cmsにおける信頼できないデータのデシリアライゼーションのぜい弱性に関する注意喚起（公開）
2025 年４月	Ivanti Connect Secure 等におけるぜい弱性（CVE-2025-22457）に関する注意喚起（公開）
	2025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）
	Active! mail におけるスタックベースのバッファオーバーフローのぜい弱性に関する注意喚起（公開）

2025年５月	2025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）
	Ivanti Endpoint Manager Mobile（EPMM）のぜい弱性（CVE-2025-4427、CVE-2025-4428）に関する注意喚起（公開）
2025年６月	Adobe Acrobat及びReaderのぜい弱性（APSB25-57）に関する注意喚起（公開）
	2025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）
2025年７月	2025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）
2025年８月	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における複数のＯＳコマンドインジェクションのぜい弱性に関する注意喚起（公開）
	2025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）
	Citrix Netscaler ADC及びGatewayのぜい弱性（CVE-2025-7775）に関する注意喚起（公開）
2025年９月	Adobe Acrobat 及び Reader のぜい弱性（APSB25-85）に関する注意喚起（公開）
	2025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）
	Cisco ASA 及び FTD における複数のぜい弱性（CVE-2025-20333、CVE-2025-20362）に関する注意喚起（公開）
2025年10月	2025 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）
2025年11月	2025 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）
2025年12月	Array Networks Array AG シリーズにおけるコマンドインジェクションのぜい弱性に関する注意喚起（公開）
	Adobe Acrobat 及び Reader のぜい弱性（APSB25-119）に関する注意喚起（公開）
	2025 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）
	WatchGuard 製 Firebox の iked における境界外書き込みのぜい弱性（CVE-2025-14733）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：2025/1/23 [2024年10月１日～2024年12月31日]
発行日：2025/4/17 [2025年１月１日～2025年３月31日]
発行日：2025/7/17 [2025年４月１日～2025年６月30日]

発行日：2025/10/16[2025 年７月１日～2025 年９月 30 日]

(3) ＪＰＣＥＲＴ／ＣＣ レポート
[発行件数] 75 件
[ぜい弱性情報の発行件数] 588 件

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取りまとめたものであり、具体的には、独立行政法人自ら又は委託による研究、国からの委託又は補助による研究である。

実施テーマは以下の４件であり、その研究開発の概要は、別添１のとおりである。

- サイバー空間の状況把握・防御技術の向上及び共通基盤の整備
- Ｗｅｂ媒介型攻撃対策技術
- サイバーセキュリティ技術の研究開発
- 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７年 12 月２日から令和８年１月 16 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７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民間企業等は次のとおりである。

ア　大学等（13 大学等、14 件）

大分大学
公立大学法人大阪
岐阜大学（２件）
埼玉工業大学
東北工業大学
東京情報大学
東京都市大学
名古屋電気学園
北海道科学大学
文理学園
前橋工科大学
宮崎大学
琉球大学

イ　民間企業（３社、５件）

株式会社 ZenmuTech
株式会社電通総研（２件）
株式会社トレードワークス（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民間企業等の中から、調査対象として無作為抽出した大学等 285 校、企業 1,599 社の計 1,884 団体を対象に実施した。

・ 大学等

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」又は「金融」であるもの

（別添１）

対象技術　侵入検知・防御技術、ぜい弱性対策技術

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 10 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等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を活用したぜい弱性の検知・評価技術、耐量子計算機暗号の実装技術、ペネトレ―ションテスト等の検証手法自動化技術等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。

情報に関する共通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を活用したぜい弱性探査技術／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及びそれら能力・技術の評価技術と評価環境の開発・展開を目指す。

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版及びモバイル版の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。基盤の安定運用に向けた改修及び体制整備を進めるとともに、ユーザ増及び定着率の向上を目的とした機能の拡張を進めた。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ともに、ユーザ増及び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　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など、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　042-327-6826

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　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及び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（耐量子計算機暗号を含む。）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部門
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及び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についてセキュリティの測定、強化及び保証をする技術を確立していく。

（別添２）

ア　大学等

企業・大学名	大分大学
代表者名	学長　北野　正剛
所在地	870-1192 大分県大分市大字旦野原７００番地
窓口部署名	研究推進部学術情報課
電話番号	097-554-7482
関連部門名	学術情報拠点（情報基盤センター）/理工学部
ホームページのURL	https://www.oita-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： 名称はない（学内の研究段階） 研究開発国： 日本 研究開発時期：	教員、学生の研究として、アクセス制御機能を随時取り上げている。

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	公立大学法人大阪
代表者名	理事長　福島　伸一
所在地	536-0025 大阪府大阪市城東区森之宮１丁目６番８５号３階
窓口部署名	大阪公立大学 教育推進課 情報学研究科支援室（中百舌鳥キャンパスB1棟1階）
電話番号	072-252-6377
関連部門名	知的ネットワーキング
ホームページのURL	https://www.omu.ac.jp/
研究説明のURL	https://tode-lab.github.io/en/
対象技術	研究開発状況
研究開発名称： フロー間の伝送機会公平性を実現するMACフレーム伝送制御 研究開発国： 日本 研究開発時期： 2023年4月1日	無線LANにおいて，システムをダウンさせるような高負荷なデータ伝送を行おうとしても，フロー間の伝送機会公平性の観点より伝送可能レートを規制することで，高負荷な伝送を抑止可能なMACフレーム伝送制御法を研究開発中であり，具体的な提案方式の設計作業を進めている．

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	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/DGXZQOGN27EC70X20C21A700000/?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	埼玉工業大学
代表者名	松川 聖業
所在地	369-0293 埼玉県深谷市普済寺1690
窓口部署名	研究支援課
電話番号	048-585-6895
関連部門名	埼玉工業大学 工学部 情報システム学科 土田研究室
ホームページのURL	https://www.sit.ac.jp
研究説明のURL	URLはありません。

対象技術	研究開発状況
研究開発名称： 関数型暗号に関する研究 研究開発国： 日本 研究開発時期： 2025年4月1日～2026年3月31日	関数型暗号とは、暗号方式単体でアクセス制御を実現する暗号技術である。今年度の卒研生が、卒業研究として関数型暗号における復号の高速化に取り組んでいる。現在は、先行研究の公開された実装を、研究室環境で動作させることに成功している。9月以降、復号処理の高速化を実現する。当該研究は卒業研究であるため、今年度中に完了する予定。

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	東北工業大学
代表者名	渡邉 浩文
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課程 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	Linuxカーネルに搭載されているeBPF（extended Berkeley Packet Filter）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．これまでに，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て蓄積するシステムを開発し，実現性を検証するとともに，性能面の課題を明らかにした．現在は，蓄積した情報を用いてホストの通信履歴をアプリケーション単位で詳細に可視化する技術の開発を進めており，その成果は不審なアプリケーションや通信の特定に寄与するものと期待される．今後は，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て，柔軟かつ細粒度なアクセス制御を実現するための技術開発を推進する．

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	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	東京都市大学
代表者名	
所在地	158-8557 東京都玉堤1-28-1
窓口部署名	総務課
電話番号	03-5707-0104
関連部門名	塩本研究室
ホームページのURL	https://www.tcu.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 連合学習、準同型暗号、分散型識別子 研究開発国： 日本 研究開発時期： 2024年4月1日～2030年3月31日	異常トラヒック検知をユースケースとして連合学習、準同型暗号、および分散型識別子を用いたセキュアデータ分析基盤ネットワークの研究に取り組んでいる。 2024～2025にかけて有効性検証の為のFeasibility Studyに取り組んでいる。FSで有効性が検証できれば、基盤ネットワークの検討に進む。

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	学校法人名古屋電気学園
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	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://pluslab.org/project_on.html
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	プロトタイプ実装は完成しており概念実証は終えています。今後は実用化に向けての設計と実装が必要な状況です。

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	北海道科学大学
代表者名	川上 敬
所在地	006-8585 札幌市手稲区前田7条15丁目4-1
窓口部署名	研究推進課
電話番号	011-688-2241
関連部門名	北海道科学大学　情報科学部　情報科学科
ホームページのURL	https://www.hus.ac.jp/
研究説明のURL	https://kaken.nii.ac.jp/grant/KAKENHI-PROJECT-25K15119/
対象技術	研究開発状況
研究開発名称： 暗号解析プロセスの自動化を実現する生成AIプロンプトの開発 研究開発国： 日本 研究開発時期： 2025年4月1日～2030年3月31日	本研究は，生成AIを活用し，軽量暗号の安全性評価プロセスを自動化することを目指す．具体的には，MILP等のプログラム作成を支援する生成AIプロンプトを開発し，その出力精度に影響を与える要素を特定し，高精度なプロンプトを開発・公開する．本研究の独自性は，生成AIを用いることで高度なプログラミングの知識や技術を必要とせず，迅速かつ正確な結果が得られることである．これにより，軽量暗号の安全性評価を促進してSociety 5.0の実現に貢献すると共に，世界の暗号研究コミュニティへの貢献を強化し，我が国の研究が国際的にリードする立場を確立する．

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	学校法人　文理学園
代表者名	菅　貞淑
所在地	870-0397 大分県大分市一木１７２７
窓口部署名	大学総務
電話番号	097-524-2700
関連部門名	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	https://researchmap.jp/manabu_fukushima
対象技術	研究開発状況
研究開発名称： 時間追従型認証技術 研究開発国： 日本 研究開発時期： 1988年4月1日～2032年3月31日	これまでに，バイオメトリクスを利用した本人認証技術を中心に取り組んできていた．しかし，１）ワンタイム認証では認証後のなりすましに対応できない，２）デジタルツインによるバイオメトリクス単独での認証の安全性が疑わしくなっている，の理由から他の目的で進めてきた研究成果をネットワークセキュリティ技術に転用することを考えた． 具体的には，1988年から取り組んでいる利用者認証からの累積成果，空間特性抽出技術として取り組んできた研究成果，発話語評価として取り組んできた研究成果，短時間高精度伝達特性変化検出として取り組んできた研究成果を，バイオメトリクス認証と統合を試みている． これにより，IDとパスワードのようなテキストデータ，ICチップのような正当保有者以外も保有できる物，指紋・性脈・顔認証のような認証後になりすまし可能な認証技術ではなしえなかった複合的かつ変化量監視による継続的な本人認証と物理的インシデント対策を可能とする認証技術の確立を目指している． 要素技術は既に学会発表等を通して公開しており，統合に向けた要素技術についても個々の成果はそれぞれの分野の学会を通して成果発表している．

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	公立大学法人前橋工科大学
代表者名	理事長　西薗　大実
所在地	371-0816 群馬県前橋市上佐鳥町460-1
窓口部署名	総務課総務企画係
電話番号	027-265-7351
関連部門名	工学部　情報システムプログラム
ホームページのURL	https://www.maebashi-it.ac.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： ソフトウェア実装によるパケット分類アルゴリズムの開発 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	ソフトウェア実装によるパケットフィルタアルゴリズムの開発を行っている。線形探索に置き換わる新しいパケットフィルタアルゴリズムの理論を構築している段階である。

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	国立大学法人宮崎大学
代表者名	鮫島　浩
所在地	889-2192 宮崎県宮崎市学園木花台西1-1
窓口部署名	企画総務部総務広報課総務
電話番号	0985-58-2854
関連部門名	工学教育研究部
ホームページのURL	https://www.miyazaki-u.ac.jp/
研究説明のURL	https://kaken.nii.ac.jp/ja/grant/KAKENHI-PROJECT-24K14948/
対象技術	研究開発状況
研究開発名称： 深層学習を用いた筋電位による多要素個人認証の複数点測定による高精度化 研究開発国： 日本 研究開発時期： 2024年4月1日～2027年3月31日	筋電位を用いた個人認証システムの実現には、予め登録されているジェスチャの波形とシステムに入力された波形を比較し、同一人物による同一のジェスチャであるか否かを判定する手法が必要である。その実現のため、以前に科研費を受けた課題（課題番号：20K11812）から継続して研究を進めている。前課題では、新型コロナウィルス感染症(COVID-19)の流行の影響により、多くの被験者からデータを取得することが困難となったため、複数人の間でジェスチャの違いを認識することよりも、単一の被験者を対象に、その被験者による複数のジェスチャを互いに識別することを優先していたた。その範囲において、さらに以前の研究（課題番号：17K11812）での、サポートベクターマシン(SVM)を中心にジェスチャ認識を行っていたが、（1）深層学習の導入と、（2）複数点計測（これまでは前腕部の掌側一箇所でのみ筋電位を測定していたものを、手の甲側、さらに両側面の計4箇所で測定し、4倍のデータを利用してジェスチャの波形比較を行う改良）の導入により、これまでより非常に大きな性能向上が見られ、国際会議での報告を行った。本課題の初年度としては、次の2つを行った。 ・前課題(20K11812)の実験で利用したのと同じ5種のジェスチャを対象として2名分の筋電位データをそろえ、それらを利用して、ジェスチャの認識実験を行なった。その結果、5種のジェスチャそれぞれについて、この二人の被験者のどちらが行なったジェスチャであるのかを、筋電位の波形を判定器に与えることによって、判別することに成功した。 ・さらなる認識精度向上を目指して、腕を動かした際の角速度を併用した認識の検討を始めた。まず、筋電位とともに腕を動かした時の角速度を同時に計測できる筋電位計（およびそれと組み合わせて使用するセンサ等）を購入し、実験にとりかかる準備を進めた。

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	
所在地	903-0213 沖縄県中頭郡西原町字千原１
窓口部署名	
電話番号	
関連部門名	工学部
ホームページのURL	
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 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	○

イ　企業

企業・大学名	株式会社Ｚｅｎｍｕ Ｔｅｃｈ
代表者名	阿部　泰久
所在地	104-0061 東京都中央区銀座8－17－5　THE HUB銀座OCT 804
窓口部署名	管理部
電話番号	03-6260-6195
ホームページのURL	https://zenmutech.com/
対象技術	技術の概要・特徴など
製品名： ZENMU Virtual Drive 開発元(メーカー名等)： ZenmuTech 開発国： 日本 価格： 1ライセンス当たり ¥1,800/月 発売時期： 2021年12月20日 出荷数：	■概要 ZENMU Virtual Driveは、PCの社外持ち出しやセキュリティ対策に関するよくある悩み・課題を解決します。 ・PCの盗難や紛失時の情報漏洩リスク ・オフライン環境での利用 ・低価格 ・管理・運用が容易 ■特徴 ・秘密分散技術による高いセキュリティ － 独自の秘密分散技術(AONT)により、ユーザーデータを無意味化した上で分散保管することでPCの紛失や情報漏洩の発生を防ぎます。 ・簡単導入 － PCにアプリをインストールし、設定するだけで利用可能。クラウド基盤を利用したサービスのため、サーバーの新規購入や設計・構築等の作業は不要です。 ・安定したパフォーマンス － ユーザーデータ以外のPCリソースはすべてローカル環境を利用するため、安定したパフォーマンスが実現可能です。 ・PC紛失時に遠隔で復元を防止 － クラウド側の分散片へのアクセスを停止するだけで元データを復元することができなくなるため、確実にデータを保護することが可能です。 ・オフライン環境での利用も可能 － オフライン機能の利用により、事前に登録したスマートフォンやUSBデバイスとの連携により、クラウド環境にアクセスできない場合でも業務継続が可能です。 ・EntraID/Okta連携 － Microsoft365等でEntraID認証を利用されている場合やOkta認証を利用されている場合には、既存のアカウント情報でログインが可能なため、新たにパスワードを発行、管理する必要がありません。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	○

企業・大学名	株式会社 電通総研
代表者名	岩本 浩久
所在地	108-0075 東京都港区港南２丁目１７番１号
窓口部署名	Open Innovationラボ
電話番号	03-6713-6111
ホームページのURL	https://www.dentsusoken.com/
対象技術	技術の概要・特徴など
製品名： VeCrea 開発元（メーカー名等）： 株式会社電通総研 開発国： 日本 価格： 発売時期： 出荷数：	

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	株式会社 電通総研
代表者名	岩本 浩久
所在地	108-0075 東京都港区港南２丁目１７番１号
窓口部署名	Open Innovationラボ
電話番号	03-6713-6111
関連部門名	OpenInnovationラボ
ホームページのURL	https://www.dentsusoken.com/
研究説明のURL	https://itsol.dentsusoken.com/vecrea/
対象技術	研究開発状況
研究開発名称： VeCrea（ヴィクレア） 研究開発国： 日本 研究開発時期： 2022年7月1日～2025年12月31日	Verifiable Credentials技術（デジタル証明書）を活用した先進的なデジタル証明書管理プラットフォーム「VeCrea」の製品化に向けた研究開発を実施中。 VeCreaは、安全で透明性の高い情報連携を実現し、ビジネスの信頼性を飛躍的に向上させる VeCreaが提供するサービス例 ①VC発行サービス 企業や組織がVCを簡単に発行できるプラットフォームを提供します。国際的な標準仕様（OID4VCI）に基づいたデジタル証明書を作成し、デジタル空間における信頼性を確立 ②VC検証サービス 受け取ったVCを容易に検証できるサービス。API＆SDKを通じて既存システムとシームレスに連携し、信頼性の高い情報を安全に活用可能 ③デジタルIDウォレット 個人や法人がVCを安全に保管・管理できるデジタルIDウォレットを提供。スマホのアプリ対応は勿論のこと、WEBにも対応。ユーザーがアプリインストール無しのスキーム構築も可能

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	株式会社トレードワークス
代表者名	代表取締役社長齋藤正勝
所在地	107-6110 東京都港区赤坂5丁目2番20号赤坂パークビル10階
窓口部署名	セキュリティサービスグループ
電話番号	03-6230-8900
ホームページのURL	https://www.tworks.co.jp
対象技術	技術の概要・特徴など
製品名： SecuAlive 開発元（メーカー名等）： 株式会社トレードワークス 開発国： 日本 価格： 規模に応じて見積 発売時期： 2012年 出荷数： 50以上	・webアプリケーション診断　・スマホアプリケーション診断　・ネットワーク診断

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	株式会社トレードワークス
代表者名	代表取締役社長齋藤正勝
所在地	107-6110 東京都港区赤坂5丁目2番20号赤坂パークビル10階
窓口部署名	セキュリティサービスグループ
電話番号	03-6230-8900
関連部門名	事業本部
ホームページのURL	htttps://www.tworks.co.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 多要素認証 研究開発国： 日本 研究開発時期： 2025年4月	汎用性の高い多要素認証基盤。一般的なパスキー・電話などの要素に加えマイナンバーカードを用いた公的認証などを総合的に管理・利用可能なサービス構築

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	