広　報　資　料
令和６年３月14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５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５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

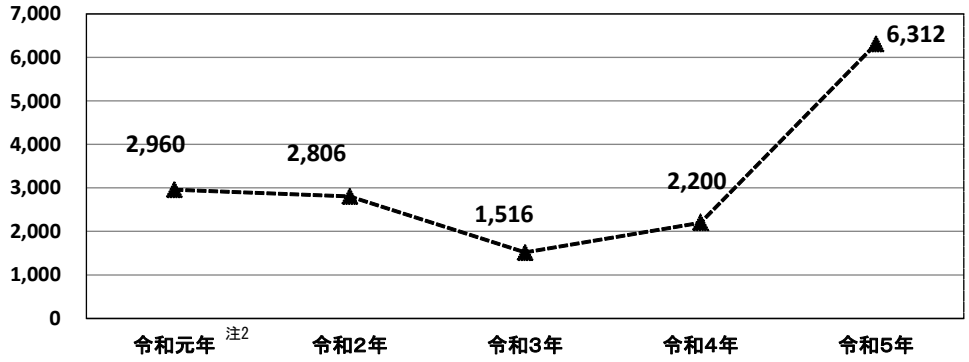
令和５年に都道府県警察から警察庁に報告がなされた不正アクセス行為の認知・検挙状況等は次のとおりである。

１　不正アクセス行為の認知状況

(1)　認知件数

令和５年における不正アクセス行為の認知件数[注1]は6,312件であり、前年（令和４年）と比べ、4,112件（約186.9%）増加した。

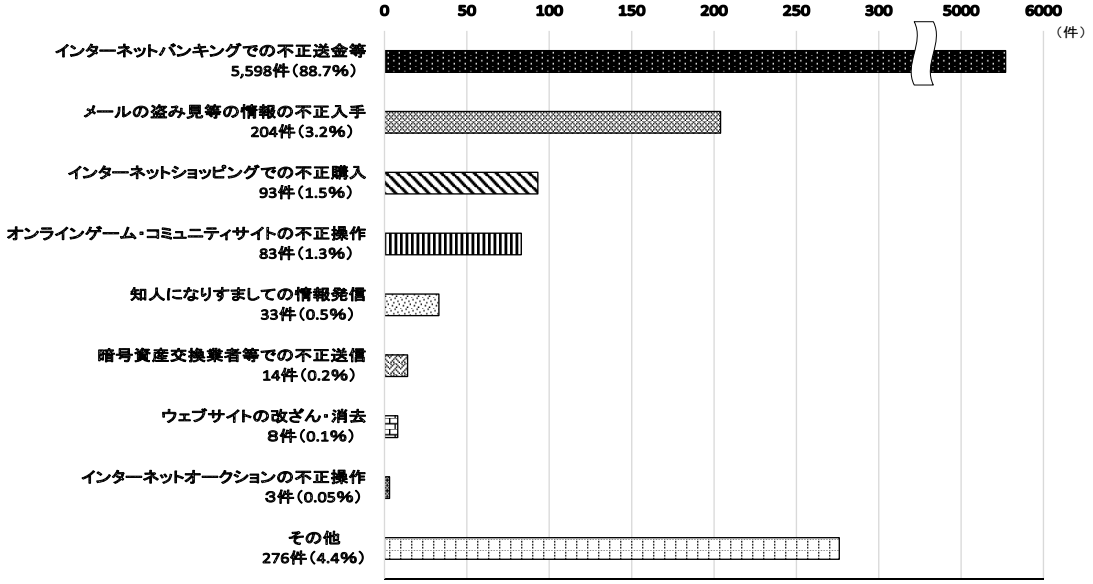
（件）　図１－１　不正アクセス行為の認知件数の推移（過去５年）



(2)　不正アクセス後の行為別の内訳

令和５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（5,598件）、次いで「メールの盗み見等の情報の不正入手」（204件）、「インターネットショッピングでの不正購入」（93件）の順となっている。

図１－２　令和５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。

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。

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	令和元年	令和2年	令和3年	令和4年	令和5年
インターネットバンキングでの不正送金等	1,808	1,847	693	1,096	5,598
メールの盗み見等の情報の不正入手	329	234	175	215	204
インターネットショッピングでの不正購入	376	172	349	227	93
オンラインゲーム・コミュニティサイトの不正操作	60	81	65	63	83
知人になりすましての情報発信	30	26	71	50	33
暗号資産交換業者等での不正送信	22	18	20	32	14
ウェブサイトの改ざん・消去	19	10	8	17	8
インターネットオークションの不正操作	47	6	4	0	3
その他	269	412	131	500	276
計	2,960	2,806	1,516	2,200	6,312

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５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521件・259人であり、前年（令和４年）と比べ、１件減少・２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487件・248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3]」が11件・８人、「識別符号提供（助長）行為[注4]」が13件・10人、「識別符号保管行為[注5]」が７件・６人、「識別符号不正要求行為[注6]」が３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		令和元年	令和2年	令和3年	令和4年	令和5年
不正アクセス行為	検挙件数	787	585	408	491	487
	検挙事件数[注7]	218	199	189	223	216
	検挙人員	222	216	227	243	248
識別符号取得行為	検挙件数	5	3	4	8	11
	検挙事件数	4	3	2	5	4
	検挙人員	4	3	2	5	8
識別符号提供(助長)行為	検挙件数	9	4	9	5	13
	検挙事件数	6	4	8	5	6
	検挙人員	9	4	8	5	10
識別符号保管行為	検挙件数	13	14	7	16	7
	検挙事件数	5	13	6	8	6
	検挙人員	7	13	6	8	6
識別符号不正要求行為	検挙件数	2	3	1	2	3
	検挙事件数	1	2	1	2	2
	検挙人員	1	5	1	2	2
計	検挙件数	816	609	429	522	521
	検挙事件数	232 (重複2)	207 (重複14)	195 (重複11)	237 (重複6)	221 (重複13)
	検挙人員	234 (重複9)	230 (重複11)	235 (重複9)	257 (重複6)	259 (重複15)

※　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3　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4　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5　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6　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7　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５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8]」が475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		令和元年	令和2年	令和3年	令和4年	令和5年
識別符号窃用型	検挙件数	785	576	398	482	475
	検挙事件数	216	190	182	215	207
セキュリティ・ホール攻撃型	検挙件数	2	9	10	9	12
	検挙事件数	2	9	8	8	10
計	検挙件数	787	585	408	491	487
	検挙事件数	218	199	189 (重複1)	223	216 (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8　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５年に検挙した不正アクセス禁止法違反事件に係る被疑者の年齢は、「20～29歳」が最も多く（103人）、次いで「14～19歳」（73人）、「30～39歳」（53人）の順となっている[注9]。

なお、令和５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10]、最年長の者は61歳であった。

図３－１　令和５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

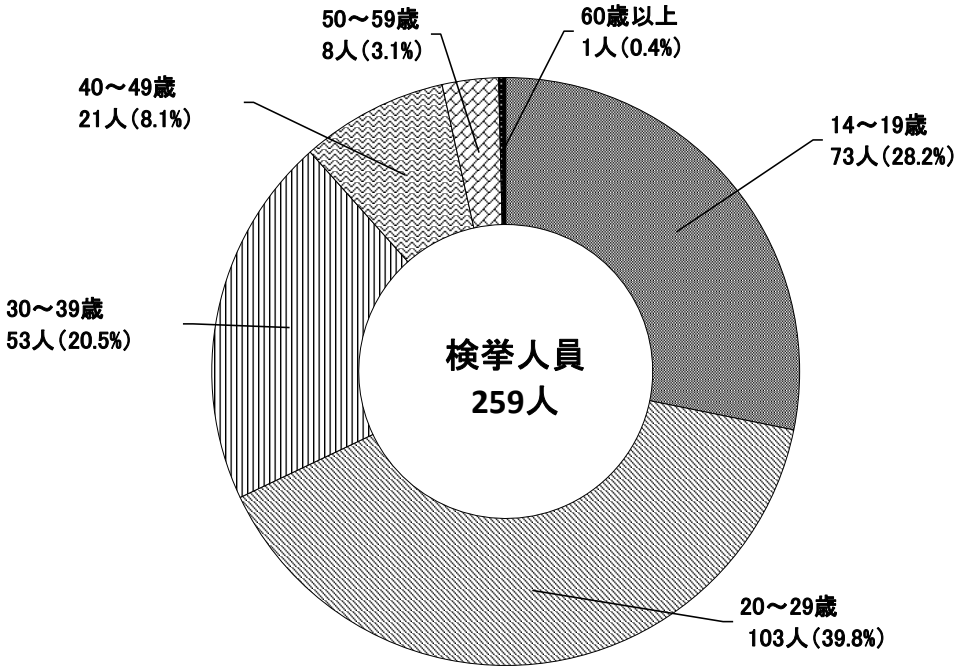


表３－１　年齢別被疑者数の推移（過去５年）

区分＼年次	令和元年	令和2年	令和3年	令和4年	令和5年
14～19歳	55	48	60	68	73
20～29歳	93	103	87	104	103
30～39歳	50	52	43	55	53
40～49歳	22	17	30	15	21
50～59歳	12	9	11	14	8
60歳以上	2	1	4	1	1
計	234	230	235	257	259

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９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５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（475件）について、そ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（203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」（68件）の順となっており、前年（令和４年）と比べ、前者は約0.88倍、後者は約1.66倍となっている。

図３－２　令和５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

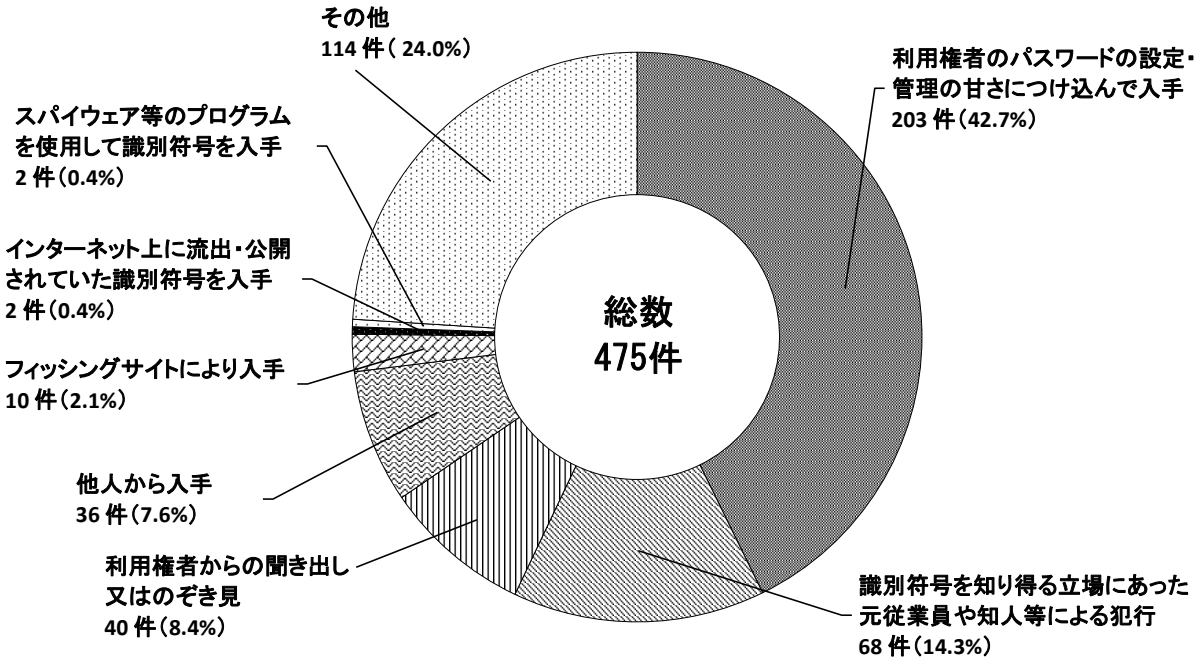


表３－２　不正アクセス行為の手口別検挙件数（過去５年）

区分＼年次	令和元年	令和2年	令和3年	令和4年	令和5年
識別符号窃用型	785	576	398	482	475
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	310	99	153	230	203
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	161	67	51	41	68
利用権者からの聞き出し又はのぞき見	20	115	36	38	40
他人から入手	182	78	34	27	36
フィッシングサイトにより入手	1	172	70	14	10
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	3	1	2	9	2
スパイウェア[注11]等のプログラムを使用して入手	5	3	0	0	2
その他	103	41	52	123	114
セキュリティ・ホール攻撃型	2	9	10	9	12

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５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（475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（234件）、次いで「社員・会員用等の専用サイト」（82件）の順となっており、前年（令和４年）と比べ、前者は約1.00倍、後者は約0.79倍となっている。

図３－３　令和５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

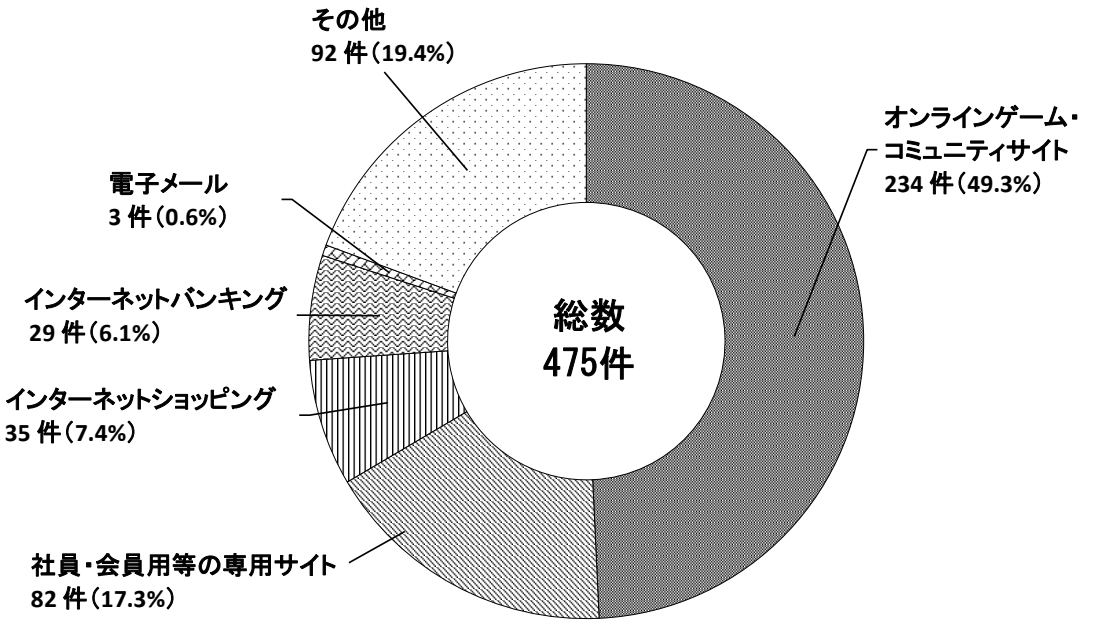


表３－３　不正アクセス行為（識別符号窃用型）により不正に利用されたサービス別検挙件数（過去５年）

区分＼年次	令和元年	令和2年	令和3年	令和4年	令和5年
オンラインゲーム・コミュニティサイト	224	88	144	233	234
社員・会員用等の専用サイト	151	174	75	104	82
インターネットショッピング	67	36	38	26	35
インターネットバンキング	14	12	96	17	29
電子メール	21	24	14	14	3
ウェブサイト公開サービス	5	1	4	8	0
インターネット接続サービス	5	1	0	1	0
インターネットオークション	4	1	0	0	0
その他	294	239	27	79	92
計	785	576	398	482	475

４　令和５年の主な検挙事例

⑴　専門学校生の男（21）は、令和４年10月及び同年12月、正規のＳＮＳになりすま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、複数の正規利用権者からＩＤ・パスワードを不正に取得した上で、取得したＩＤ・パスワードを用いて同ＳＮＳに不正アクセスした。令和５年４月、男を不正アクセス禁止法違反（不正アクセス行為、識別符号不正要求行為及び識別符号取得行為）及び私電磁的記録不正作出・同供用罪で検挙した。

⑵　公務員の女（30）は、令和４年12月、他人の個人番号カードの暗証番号を名義人に無断で設定し、設定した暗証番号を用いて不正アクセスした上で、自己が利用するキャッシュレス決済サービスにポイントを付与した。令和５年４月、女を公電磁的記録不正作出・同供用罪、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。

⑶　専門学校生の男（18）は、令和５年３月、ゲームアカウント売買サイトの利用者にゲームアカウントの購入を持ちかけ、言葉巧みに購入希望者の同サイトに係る識別符号を入手した上、同サイトに不正アクセスして同人が保有するポイントを不正に取得した。同年７月、男を不正アクセス禁止法違反（不正アクセス行為）及び電子計算機使用詐欺罪で検挙した。

⑷　会社員の男（25）は、令和４年８月から同年11月までの間、複数のＳＮＳアカウントに対し、パスワードを推測して不正アクセスした上、危害を加える旨のメッセージを正規利用権者になりすまして送信した。令和５年８月、男を不正アクセス禁止法違反（不正アクセス行為）及び脅迫罪で検挙した。

⑸　会社員の男（43）は、令和３年６月、元勤務先の名刺管理システムについて従業員に割り当てられた識別符号を、転職先の同僚に提供した上、自身も同システムに不正アクセスをした。令和５年９月、男を個人情報保護法違反、不正アクセス禁止法違反（不正アクセス行為）で検挙した。

⑹　無職の男（20）ほか２名は、共謀の上、令和５年１月、ＳＮＳ事業者が運営するウェブサイトであると誤認させるウェブサイトを海外サーバに記録蔵置し、正規利用権者にパスワード等を入力することを求める旨の情報を不特定多数の者が閲覧できる状態に置いた。令和５年９月、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。

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12]や二経路認証[注13]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12　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13　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。

⑵　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。

⑶　ＩＤ・パスワードの適切な管理

ＩＤ・パスワードを知り得る立場にあった元従業員、委託先業者等の者による不正アクセス行為が発生していることから、利用権者が特定電子計算機を利用する立場でなくなった場合には、アクセス管理者が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。

⑷　セキュリティ・ホール攻撃への対策

ウェブシステムやＶＰＮ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。

⑸　フィッシング等への対策

フィッシング等により取得したＩＤ・パスワード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。

（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５年（令和５年１月１日から令和５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４年：226 件）であった（注２）。令和５年は令和４年と比べて、17 件（約 7.5%）増加した。

届出の被害内容で主に見受けられたものは、令和４年に引き続き、VPN 装置の脆弱性を悪用した不正侵入によるランサムウェア攻撃（データを暗号化しない攻撃も含む)、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情報窃取、そしてリスト型攻撃や総当たり攻撃等により、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 698 件（令和４年：655 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 512 件（令和４年：525 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。

187 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）：79 件

脆弱性を悪用した攻撃：62 件
システムの設定不備を悪用した攻撃：46 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。320 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：168 件
不正プログラムの埋め込み：95 件
資源利用(CPU 等のリソース不正使用)：48 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、４件（令和４年：７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。182 件（令和４年：123 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：102 件
ソーシャルエンジニアリング：17 件
不審メール（スパムメール、フィッシングメール、SMS 等）：８件

(2) 原因別分類
243 件の届出のうち、実際に被害に遭った 186 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 206 件（令和４年：216 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令和４年に引き続き多かった。これはコロナ禍の中、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 環境を構築後、VPN 装置や VPN 機能を有するネットワーク機器の維持・保守に係る運用方針が未だに定まらない状態で運用を続けるなどした結果、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多く、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：48 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）：42 件
原因不明：39 件
ID、パスワード管理の不備：26 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：92 件
メールサーバ：50 件
クライアント：49 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 486 件（令和４年：494 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】
ファイルの書き換え：96 件
データの窃取や盗み見：84 件
不正プログラムの埋め込み：79 件

(5) 対策情報
冒頭で述べた通り、令和５年においても VPN 装置の脆弱性を悪用した不正侵入によるランサムウェア攻撃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 206 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

23.3%（48 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 20.4%（42 件）であり、この２つの項目で約 43.7%（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 12.6%（26 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、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を勧める。

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】

「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

「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/

「IPA メールニュース」
https://www.ipa.go.jp/mailnews.html

【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/
「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５年（令和５年１月１日から令和５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 65,669 件であった。この報告を元にしたインシデント件数（注３）は 28,735 件であり、インシデントをカテゴリ別に分類すると以下の通りである。

（１）　プローブ、スキャン、その他不審なアクセスに関する報告

防御に成功したアタックや、コンピュータ／サービス／弱点の探査を意図したアクセス、その他の不審なアクセス等、システムのアクセス権において影響を生じないか、無視できるアクセスについて 5,089 件の報告があった。

[1/1-3/31: 2,059 件、4/1-6/30: 998 件、7/1-9/30: 639 件、10/1-12/31: 1,393 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 869 件の報告があった。

[1/1-3/31: 362 件、4/1-6/30: 97 件、7/1-9/30: 89 件、10/1-12/31: 72 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 393 件の報告があった。

[1/1-3/31: 154 件、4/1-6/30: 97 件、7/1-9/30: 89 件、10/1-12/31: 53 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 21 件の報告があった。

[1/1-3/31: 9 件、4/1-6/30: 8 件、7/1-9/30: 3 件、10/1-12/31: 1 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 20,966 件の報告があった。
[1/1-3/31: 5,553 件、4/1-6/30: 6,186 件、7/1-9/30: 4,754 件、10/1-12/31: 4,473 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 1 件の報告があった。
[1/1-3/31: 0 件、4/1-6/30: 1 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 10 件の報告があった。
[1/1-3/31: 3 件、4/1-6/30: 4 件、7/1-9/30: 2 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 1,386 件の報告があった。
[1/1-3/31: 319 件、4/1-6/30: 320 件、7/1-9/30: 292 件、10/1-12/31: 455 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]

公開月	注意喚起内容
2023 年 1 月	2023 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）
	Adobe Acrobat および Reader の脆弱性（APSB23-01）に関する注意喚起（公開）
	2023 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）
2023 年 2 月	2023 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）
2023 年 3 月	マルウェア Emotet の感染再拡大に関する注意喚起（更新）
	2023 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）
	マルウェア Emotet の感染再拡大に関する注意喚起（更新）
	2023 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（更新）
	2023 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（更新）
	マルウェア Emotet の感染再拡大に関する注意喚起（更新）
2023 年 4 月	2023 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）
	Adobe Acrobat および Reader の脆弱性（APSB23-24）に関する注意喚起（公開）
	2023 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）
2023 年 5 月	2023 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）
2023 年 6 月	2023 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）
2023 年 7 月	2023 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）
	Citrix ADC および Citrix Gateway の脆弱性（CVE-2023-3519）に関する注意喚起（公開）
	2023 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）
	Citrix ADC および Citrix Gateway の脆弱性（CVE-2023-3519）に関する注意喚起（更新）
2023 年 8 月	Proself の認証バイパスおよびリモートコード実行の脆弱性に関する注意喚起（公開）
	2023 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）
	Adobe Acrobat および Reader の脆弱性（APSB23-30）に関する注意喚起（公開）
	Proself の認証バイパスおよびリモートコード実行の脆弱性に関する

	注意喚起（更新）
	Citrix ADC および Citrix Gateway の脆弱性（CVE-2023-3519）に関する注意喚起（更新）
	Proself の認証バイパスおよびリモートコード実行の脆弱性に関する注意喚起（更新）
2023 年 9 月	Barracuda Email Security Gateway（ESG）の脆弱性（CVE-2023-2868）を悪用する継続的な攻撃活動に関する注意喚起（公開）
	2023 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（APSB23-34）に関する注意喚起（公開）
	Array Networks Array AG シリーズの脆弱性を悪用する複数の標的型サイバー攻撃活動に関する注意喚起（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における任意のコード実行の脆弱性に関する注意喚起（公開）
	Array Networks Array AG シリーズの脆弱性を悪用する複数の標的型サイバー攻撃活動に関する注意喚起（更新）
2023 年 10 月	Proself の XML 外部実体参照（XXE）に関する脆弱性を悪用する攻撃の注意喚起（公開）
	2023 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）
	Citrix ADC および Citrix Gateway の脆弱性（CVE-2023-3519）に関する注意喚起（更新）
	Cisco IOS XE の Web UI における権限昇格の脆弱性（CVE-2023-20198）に関する注意喚起（公開）
	2023 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）
	Proself の XML 外部実体参照（XXE）に関する脆弱性を悪用する攻撃の注意喚起（更新）
	Citrix ADC および Citrix Gateway の脆弱性（CVE-2023-4966）に関する注意喚起（公開）
	Cisco IOS XE の Web UI の脆弱性(CVE-2023-20198)に関する注意喚起（更新）
	Proself の XML 外部実体参照（XXE）に関する脆弱性を悪用する攻撃の注意喚起（更新）
2023 年 11 月	2023 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）
	Adobe Acrobat および Reader の脆弱性（APSB23-54）に関する注意喚起（公開）
	日本の組織を標的にした外部からアクセス可能な IT 資産を狙う複数の標的型サイバー攻撃活動に関する注意喚起（公開）
	Citrix ADC および Citrix Gateway の脆弱性（CVE-2023-4966）に関する注意喚起（更新）
2023年12月	2023 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：2023/1/19［2022 年 10 月 1 日～2022 年 12 月 31 日］
発行日：2023/5/12［2023 年 1 月 1 日～2023 年 3 月 31 日］
発行日：2023/7/13［2023 年 4 月 1 日～2023 年 6 月 30 日］
発行日：2023/10/17[2023 年 7 月 1 日～2023 年 9 月 30 日］

（３） JPCERT/CC レポート

［発行件数］83 件
［脆弱性情報の発行件数］474 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。

- 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
- サイバーセキュリティ技術の研究開発
- 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
- エマージング技術に対応したダイナミックセキュアネットワーク技術の研究開発
- 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５年12月４日から令和６年１月19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件でした。

(2)　調査

警察庁が令和５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（８大学、13件）

神奈川工科大学
佐賀大学（２件）
諏訪東京理科大学
東北工業大学
名古屋大学
日本大学（４件）
福岡大学（２件）
横浜国立大学

イ　企業（４社、14件）

株式会社ＳＲＡ（５件）
トレンドマイクロ株式会社
株式会社ヌーラボ
三菱電機株式会社（７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５年度

実施主体　ウエステルスコンサルティング株式会社（警察大学校が実施する委託研究の委託先）

法人番号　2011001106948

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）

１　調査

(1)　偽造指紋、顔影像等スマートフォンのロック機能解除に際し現実的に想定される脅威

(2)　当該脅威に対応し、我が国国内の市場等を通じて既に入手可能な生体認証評価技術

２　実現可能な手法の検討及び提案

１の調査結果に基づき、科学的に信頼できる耐偽造能力評価手法を提案する。ただし、追加の技術開発が必要な場合、その実現可能性を検討する。

３　提案手法の実証と実態把握

実際に、市場に投入される指紋、顔画像等生体認証技術を利用するモバイル機器等製品について、２の手法を適用し、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

市場に流通するスマートフォン等を対象に、手口の有効性等の実態を把握し、その結果に基づき、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　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　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　侵入検知・防御技術

テーマ名　エマージング技術に対応したダイナミックセキュアネットワーク技術の研究開発

開発年度　令和３年度～令和４年度

実施主体　アラクサラネットワークス株式会社、学校法人慶應義塾他

法人番号　4020001077949（アラクサラネットワークス株式会社）、4010405001654（学校法人慶應義塾）他

背景、目的

Beyond 5G時代の通信網には、多種多様な機器が接続され、電波資源の有効活用のためには、無駄な通信を排除し通信網全体での高度セキュア化が必要である。光通信技術による帯域と距離の克服を利用して、限られた計算資源・人的資源を効率的に利活用してセキュアネットワークを実現する。

研究開発状況（概要）

プログラマブルノード（ネットワークセンサ）技術、セキュアな広域低遅延通信実現をサポートする高度プロービング技術、デジタルツイン監視を実現するためのAPIによるIn-Network Security技術、の研究開発を行う。

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_02501.html）
電話 042－327－6011

将来の方向性

開発した技術をキャンパス網やテストベッド網での概念実証を通じて有効性を検証し、セキュアネットワークの観点からの電波資源の有効利用に寄与する。

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、暗号化した状態で検索や計算を行う秘密計算技術（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、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）

ア　大学

企業・大学名	神奈川工科大学
代表者名	小宮山　一三
所在地	243-0292 神奈川県厚木市下荻野1030
窓口部署名	研究推進機構 広報部門
電話番号	046-291-3109
関連部門名	神奈川工科大学　研究推進機構
ホームページのURL	https://www.kait.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： セキュリティー研究センター 研究開発国： 日本 研究開発時期： 2021年3月～2024年8月	「分散型機械学習モデルに基づいた安全なIoTサービスを実現するための統合セキュリティー対策技術に関する研究」 本研究の目的は、誰もが安心して暮らせる超スマートな社会を実現するために、フィジカル空間とサイバー空間を融合したすべての部分で安全性と信頼性を確保することができる高度かつ検漏なIoTセキュリティー総合対策を確率する事である。　具体的には、超スマート社会実現におけるサイバー攻撃の脅威を明確に分析し、フィジカル空間からサイバー空間まで一貫して安全性を提供可能となる高度なIoTセキュリティーシステム構築技術の確立について検討する。　そして、不正デバイスと不正アップリケ―ションを見分けることができるデバイス認証技術とユーザー認証技術を開発するとともに、不正データ・異常データをより早く検知することができる信頼性の高い分散機械学習モデル構築手法の研究開発を行う。 今年度は、これまで検討・提案してきたスマートフォンとスマートウオッチのようなウエアラブル端末を用いた個人認証方式の有効性を検討する。　さらに、スマートフォンの行動的特徴量による個人識別に関する検討と文章作成中の打鍵情報による継続的な本人認証について検討を行っている。

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	国立大学法人佐賀大学
代表者名	兒玉浩明
所在地	840-8502 佐賀市本庄町１番地
窓口部署名	佐賀大学総合情報基盤センター
電話番号	0952-28-8149
ホームページのURL	https://www.saga-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： Opengate 開発元(メーカー名等)： 佐賀大学 開発国： 日本 価格： 無償 発売時期： 2005年 出荷数： 不明（ウェブサイトで公開）	背景： インターネットが社会に浸透してきた現在、携帯型コンピュータを接続できる情報コンセントや多人数共用の公開端末など、ネットワーク利用環境を広 く整備することが要望されている。一方、インターネット上では、侵入破壊行為や誹謗中傷行為等のトラブルが頻発しており、公開端末や情報コンセン ト等を無制限で開放することは許されなくなっている。しかし、公開端末ではシステムの認証機構不足や管理負担のため、また情報コンセントでは利用者本人が所有する機器を対象とするため、適切な認証を一律に適用することは困難である。 目的： 公開端末や情報コンセント・無線LAN等においても、利用資格を持つ者のみがネットワークを利用できるように制限するとともに、トラブル時の個人 特定を可能とするシステムの構築を目的とする。 利用： ブラウザを立ち上げて任意のサイトをアクセスする。すると認証要求ページが送られてくるので、ユーザIDとパスワードを返答する。許可ページ が表示されればネットワークが利用できる。ブラウザを終了するとネットワークが閉鎖される。 機能と構成： 本システムは、端末群と利用ネットワークとの間にゲートウエイを設置し、そこを通過するパケットをフィルタリングするシステムとして実現する。 端末にはWebブラウザが必要である。OS等は特に制限しない。また事前設定も不要である。ゲートウェイには、Webサーバとファイアウオー ルソフトが必要である。現状のプログラムは、FreeBSD上のApacheとipfwを利用している。また利用者認証のためには、FTP, POP3, POP3S, FTPS, RADIUS, LDAP, PAM, Shibboleth, HttpBasicをサポートしている。Opengateは CGIとして起動し、端末にAjaxスクリプトを送り、ブラウザの生存を監視する。

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	国立大学法人佐賀大学
代表者名	兒玉浩明
所在地	840-8502 佐賀市本庄町１番地
窓口部署名	佐賀大学総合情報基盤センター
電話番号	0952-28-8149
関連部門名	理工学部電気電子工学部門
ホームページのURL	https://www.saga-u.ac.jp/
研究説明のURL	http://www.bioengineering.saga-u.ac.jp/research/douzono.html
対象技術	技術の概要・特徴など
研究開発名称： 身体的特徴量、行動的特徴量、知識を組み合わせた認証方式の開発 研究開発国： 日本 研究開発時期： 1996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	公立大学法人公立諏訪東京理科大学
代表者名	北原　政彦
所在地	391-0292 長野県茅野市豊平5000-1
窓口部署名	事務局総務課
電話番号	0266-73-1201
ホームページのURL	https://www.sus.ac.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： Fortigate 50OE 開発元(メーカー名等)： Fortinet 開発国： アメリカ 価格： 830万円（本体のみの価格） 発売時期： 2018年3月1日 出荷数： 不明	FortiGate 50OE シリーズは、中規模から大規模の企業向けに次世代ファイアウォール（NGFW）機能を提供します。キャンパスや大規模企業の支社への展開に最適な柔軟性も備えています。独自の強力なセキュリティプロセッサによって、ネットワークパフォーマンスの最適化、セキュリティの有効性、詳細な可視性が実現しており、巧妙なサイバー脅威からお客様を保護します。フォーティネットのセキュリティ ドリブン ネットワーキングのアプローチにより、新世代のセキュリティがネットワークへと緊密に統合されます。

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	技術の概要・特徴など
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eBPF(extended Berkley Packet Filter)に着目しており，eBPFを利用したアイディアの実現性の検証を進めている状況にある.

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	技術の概要・特徴など
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。 - 悪性通信の解析/検知 - HTTP(S)通信を使うC&C通信の検出 - FPGAを利用した悪性通信からの特徴量抽出 - 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 - APIコールログからのマルウェアプロセス推定 - 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 - SRv6による組織内ネットワークにおける攻撃由来通信の隔離ネットワーク誘導 - 自動リンク処理などにおける国際化ドメイン名などのセキュリティ問題 - 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 - ハニーポット通信ログ解析からのIDSシグネチャ自動選択 - 標的型攻撃対策 - 攻撃者の意図の解析を目的としたOpenFlowによる組織内感染端末通信の解析用仮想環境への誘導 - 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 - MalGANと強化学習による本命の検知率を低下させる学習用おとりマルウェアデータ生成 - 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

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： 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	理工学部応用情報科学科
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	学校法人福岡大学
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	
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	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～2024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	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	技術の概要・特徴など
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８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昨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	

イ　企業

企業・大学名	株式会社ＳＲＡ
代表者名	平田淳史
所在地	171-0022 東京都豊島区南池袋2丁目32番8号
窓口部署名	プロダクトサービス事業部
電話番号	03-5979-2111
ホームページのURL	https://www2.sra.co.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： Cavirin 開発元(メーカー名等)： Cavirin Systems, Inc 開発国： United States 価格： 月額150,000円～ 発売時期： 2018年1月 出荷数： 非公開	・ Cavirin は CSPM 領域の製品で、クラウドにおける不適切な設定、人為的な設定ミスによるリスクを監視・修復する製品 ・ CSPM 製品ですが、オンプレミスの OS・コンテナの脆弱性対策・コンプライアンス準拠を監視可能 ・ NIST, CIS, PCI DSS、HIPPA 等、複数の基準で監視可能

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ＳＲＡ
代表者名	平田淳史
所在地	171-0022 東京都豊島区南池袋2丁目32番8号
窓口部署名	プロダクトサービス事業部
電話番号	03-5979-2111
ホームページのURL	https://www2.sra.co.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： セキュリティ診断サービス 開発元(メーカー名等)： SRA 開発国： 日本 価格： 50万円～(ライト/128IP) 発売時期： 2020年～ 出荷数：	・Nessusを用いた外部(インターネット)からの脆弱性診断サービス ・複数拠点の診断も可能 ・128 IP まで同一価格(以降64IP単位) ・対象IP数と診断回数のシンプルな価格体系 ・2種類(スタンダード、ライト)の診断タイプ(日本語による診断報告書の有無) ・無償での再診断可

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ＳＲＡ
代表者名	平田淳史
所在地	171-0022 東京都豊島区南池袋2丁目32番8号
窓口部署名	プロダクトサービス事業部
電話番号	03-5979-2111
ホームページのURL	https://www2.sra.co.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： セキュリティ運用サービス 開発元(メーカー名等)： SRA 開発国： 日本 価格： 20万円～（初期費用別途） 発売時期： 2022年～ 出荷数：	・セキュリティの専門知識をもった人材による運用サービス ・24x365の運用体制 ・マルチベンダーサポート(メーカー限定無し) ・アラートなどの検知の報告のみではなく、セキュリティ向上のための設定変更などのご提案も可能 ・オプションにてパッチ適用作業やWebアプリケーション脆弱性診断なども実施可

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ＳＲＡ
代表者名	平田淳史
所在地	171-0022 東京都豊島区南池袋2丁目32番8号
窓口部署名	プロダクトサービス事業部
電話番号	03-5979-2111
ホームページのURL	https://www2.sra.co.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： セキュリティ情報提供サービス 開発元(メーカー名等)： SRA 開発国： 日本 価格： 40万円～(初期＋年額) 発売時期： 2020年～ 出荷数：	・お客様環境にあったプロダクトを選択し、ピンポイントに脆弱性情報を収集 ・CVSS評価値や危険度レベル、影響範囲などのフィルタを用いて必要な情報のみ厳選して取得することが可能

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ＳＲＡ
代表者名	平田淳史
所在地	171-0022 東京都豊島区南池袋2丁目32番8号
窓口部署名	プロダクトサービス事業部
電話番号	03-5979-2111
関連部門名	プロダクトサービス事業部
ホームページのURL	https://www2.sra.co.jp/
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： FIDO/WAF連携システム構築 研究開発国： 日本 研究開発時期： 2022年10月1日～2023年12月31日	昨年度POCと市場調査を実施し、有効と判断しため、製品化開発中。

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	トレンドマイクロ株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： Trend Vision One 開発元(メーカー名等)： トレンドマイクロ株式会社 開発国： アメリカ合衆国 *CBP(米国国土安全保障省 税関・国境取締局）の規定 に基づき、「ソフトウェアがオブジェクトコードに変換される場所」を製造国（Country of Origin）と定義しています 価格： 弊社営業までお問合せください 発売時期： 2021年3月 出荷数： 非公開	トレンドマイクロが提供するXDR（Extended Detection and Response）は、エンドポイントに加え、メール、サーバ、クラウドワークロード、ネットワーク等の複数のセキュリティレイヤから正・不正問わずファイルやプロセスに対するアクティビティデータであるテレメトリを収集し、サイバー攻撃の有無や対処すべき事項を見出します。 Trend Vision Oneでは、法人組織が平時からリスクの把握、評価、軽減を行う「アタックサーフェスリスクマネジメント」とマルウェア等の脅威や、脅威とは断定できない不審な挙動の抽出を行い、影響範囲や感染経路の特定、攻撃の全体像の可視化など、迅速な対処を行うことを支援する「XDR」を提供します。 詳細は以下をご覧ください https://www.trendmicro.com/ja_jp/business/products/one-platform.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	株式会社ヌーラボ
代表者名	橋本正徳
所在地	810-0041 福岡県福岡市中央区大名1丁目8-6 HCC BLD.
窓口部署名	情報統括部品質保証課
電話番号	092-752-5231
ホームページのURL	https://nulab.com
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： Nulab Pass 開発元(メーカー名等)： 株式会社ヌーラボ 開発国： 日本 価格： ¥990～ 発売時期： 2020年8月4日 出荷数：	Nulab Pass（ヌーラボパス）は、株式会社ヌーラボが提供するサービス（Backlog、Cacoo、Typetalk）を利用する際のセキュリティとガバナンスを強化するサービスです。 組織の管理者による統合的なアカウント管理、SAML認証によるシングルサインオン、組織のメンバーの操作を記録する監査ログを提供します。

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	三菱電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： Camellia 開発元(メーカー名等)： NTTと三菱電機による共同開発 開発国： 日本 価格： オープン 発売時期： 2000年3月10日 出荷数： 不明	Camellia（カメリア）は、世界のトップクラスの暗号研究者を抱えるNTTと三菱電機が共同で2000年に開発した共通鍵ブロック暗号です。技術的に高い安全性を有するのは当然のこと、効率性と実用性にも優れており、さまざまなプラットフォーム上でのソフトウェアによ り高速に実装することができます。ハードウェア実装においても、高速実装はもとよりコンパクトかつ低消費電力型の実装が可能です。 これらの技術的優位性は、例えば欧州連合推奨暗号選定プロジェクトNESSIEにおいて「米国政府標準暗号AESと多くの点で同等の安全性と性能を有している」と評価されるなど、国際的にも認められています。現在では、AESと同等の安全性・処理性能を有しているほぼ唯一 の暗号として国際的にも認知されつつあり、多くの国際的な標準暗号・推奨暗号に選定されています。 とりわけ、日本国産暗号としては、初めてインターネット標準暗号（IETF Standard Track RFC）として承認されました。 また、オープンソースの提供も積極的に実施しており、現在では国産暗号としては初めてOpenSSL, Firefox, Linux, FreeBSDをはじめとする国際的にも主要なオープンソースソフトウェアに搭載されています。さらには欧米企業等との連携を促進するため、NTTはMITケルベロスコンソーシアムへ加盟しました。 出典 https://info.isl.ntt.co.jp/crypt/camellia/intro.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	三菱電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： MistyGuard<CERTMANAGER> 開発元(メーカー名等)： 三菱電機インフォメーション システムズ 開発国： 日本 価格： オープン 発売時期： 2010年4月1日 出荷数： 不明	特定認証業務に対応する高度なセキュリティ運用機能、IoT機器利用に適した証明書発行、失効API機能を提供し、大規模の公的認証基盤やIoT運用基盤から中規模の企業内プライベートPKI利用システムまで様々な用途に応じた利用が可能です。 弊社MistyGuardシリーズの電子署名製品と組み合わせることで、電子証明書を利用した電子契約、電子認証等のセキュリティシステムを構築できます。 出典 https://www.mdis.co.jp/service/certmanager/

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	三菱電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： IoTハニーポット 開発元(メーカー名等)： 三菱電機 開発国： 日本 価格： 発売時期： 出荷数： 不明	IoT機器への攻撃動向を観察するためのハニーポット 販売目的で研究開発しているわけではないため、価格・発売時期等は記載しません。

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	三菱電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報技術総合研究所
ホームページのURL	
研究説明のURL	https://www.mitsubishielectric.co.jp/corporate/randd/list/info_tel/a41/index.html
対象技術	技術の概要・特徴など
研究開発名称： 認証暗号アルゴリズム 研究開発国： 日本 研究開発時期： 2018年～	「MACアルゴリズム」では共通鍵を使って送信者は改ざん検知用のタグを生成し、データとともに送信します。受信者も受け取ったデータと共通鍵を使ってタグを生成します。両方のタグを照合し、もしその内容が異なっていれば、送信の途中で第三者によってデータに手が加えられたことになり、改ざんを検知できます。 「認証暗号アルゴリズム」はタグによる改ざん検知に加え、秘匿機能を備えています。利用モードでは長いデータを扱うために、1つのデータを複数のブロックに分けて処理します。その際に暗号化毎に異なる値（ナンス）を加えて暗号化します。通常、仮にブロック1とブロック2が同じ平文であった場合、暗号文も同じになるため、第三者から見て同じ平文が続いていると推察でき、データの内容を知るヒントになりかねません。ナンスを加えて暗号化することで、同じ平文が続いても違った暗号文が出力されるため、同じ平文を繰り返し使った場合に起こりうる危険を回避でき、安全性が担保できます。

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	三菱電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報技術総合研究所
ホームページのURL	
研究説明のURL	https://www.mitsubishielectric.co.jp/corporate/special/convention/ceatec2021/cryptography/
対象技術	技術の概要・特徴など
研究開発名称： 耐量子計算機暗号 研究開発国： 日本 研究開発時期： 2018年～	格子暗号と同種写像暗号について安全性を向上したアルゴリズムを開発中

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	三菱電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報技術総合研究所
ホームページのURL	
研究説明のURL	https://www.mitsubishielectric.co.jp/corporate/randd/list/info_tel/a29/index.html
対象技術	技術の概要・特徴など
研究開発名称： 秘匿検索(検索可能暗号) 研究開発国： 日本 研究開発時期： 2016年～	基本方式の開発は完了し、システム化のためのライブリや鍵管理方式、高速化・効率化の検討を継続

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	三菱電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報技術総合研究所
ホームページのURL	
研究説明のURL	https://www.mitsubishielectric.co.jp/corporate/randd/list/info_tel/b242/index.html
対象技術	技術の概要・特徴など
研究開発名称： センサーセキュリティ 研究開発国： 日本 研究開発時期： 2019～	センサーへの攻撃手法の解析と、その解析結果を元にした攻撃対策を研究。攻撃手法と対策を評価するためのシミュレータを開発。

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	○