別紙

令和５年３月16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４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４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

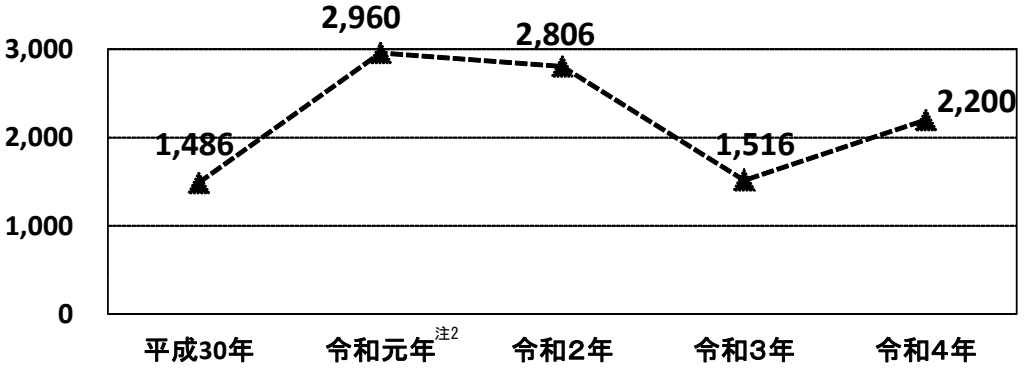
令和４年に都道府県警察から警察庁に報告がなされた不正アクセス行為の認知・検挙状況等は次のとおりである。

１　不正アクセス行為の認知状況

(1)　認知件数

令和４年における不正アクセス行為の認知件数[注1]は2,200件であり、前年（令和３年）と比べ、684件（約45.1%）増加した。

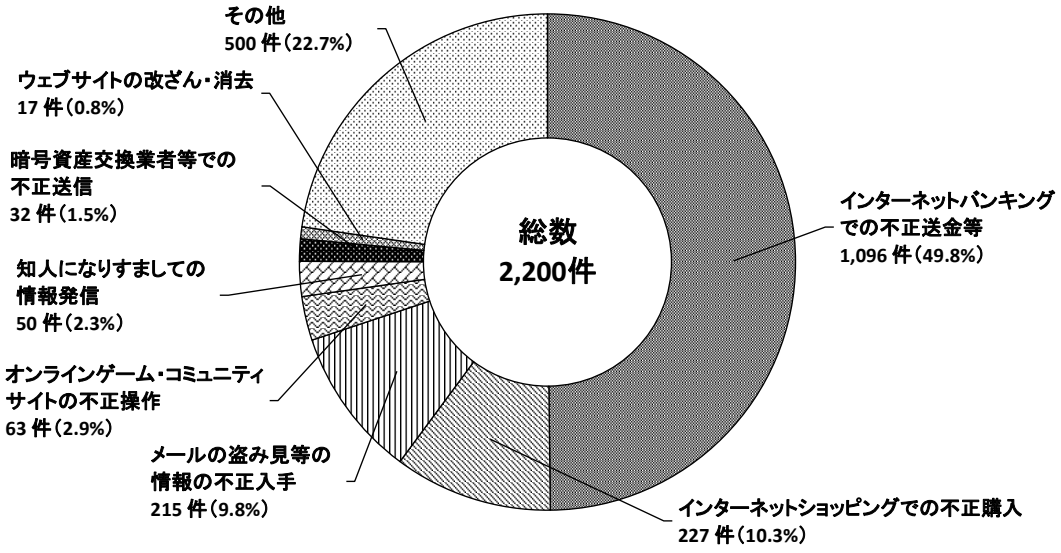
図１－１　不正アクセス行為の認知件数の推移（過去５年）



(2)　不正アクセス後の行為別の内訳

令和４年における不正アクセス行為の認知件数について、不正アクセス後に行われた行為別に内訳を見ると、「インターネットバンキングでの不正送金等」が最も多く(1,096件)、次いで「インターネットショッピングでの不正購入」(227件)、「メールの盗み見等の情報の不正入手」（215件）の順となっている。

図１－２　令和４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被疑者の行為の数をいう。

注2　令和元年の各種数値については、平成31年１月から４月までの数を含む。

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	平成30年	令和元年	令和2年	令和3年	令和4年
インターネットバンキングでの不正送金等	330	1,808	1,847	693	1,096
インターネットショッピングでの不正購入	149	376	172	349	227
メールの盗み見等の情報の不正入手	385	329	234	175	215
オンラインゲーム・コミュニティサイトの不正操作	199	60	81	65	63
知人になりすましての情報発信	24	30	26	71	50
暗号資産交換業者等での不正送信	169	22	18	20	32
ウェブサイトの改ざん・消去	13	19	10	8	17
インターネットオークションの不正操作	29	47	6	4	0
その他	188	269	412	131	500
計	1,486	2,960	2,806	1,516	2,200

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４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522件・257人であり、前年（令和３年）と比べ、93件・22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491件・243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８件・５人、「識別符号提供（助長）行為[注4]」が５件・５人、「識別符号保管行為[注5]」が16件・８人、「識別符号不正要求行為[注6]」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		平成30年	令和元年	令和2年	令和3年	令和4年
不正アクセス行為	検挙件数	520	787	585	408	491
	検挙事件数[注7]	160	218	199	189	223
	検挙人員	164	222	216	227	243
識別符号取得行為	検挙件数	22	5	3	4	8
	検挙事件数	1	4	3	2	5
	検挙人員	2	4	3	2	5
識別符号提供(助長)行為	検挙件数	4	9	4	9	5
	検挙事件数	4	6	4	8	5
	検挙人員	4	9	4	8	5
識別符号保管行為	検挙件数	16	13	14	7	16
	検挙事件数	9	5	13	6	8
	検挙人員	12	7	13	6	8
識別符号不正要求行為	検挙件数	2	2	3	1	2
	検挙事件数	2	1	2	1	2
	検挙人員	2	1	5	1	2
計	検挙件数	564	816	609	429	522
	検挙事件数	170 (重複6)	232 (重複2)	207 (重複14)	195 (重複11)	237 (重複6)
	検挙人員	173 (重複11)	234 (重複9)	230 (重複11)	235 (重複9)	257 (重複6)

※　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４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482件と全体の90%以上を占めている。

表２－２　不正アクセス行為の手口別検挙件数等（過去５年）

区分＼年次		平成30年	令和元年	令和2年	令和3年	令和4年
識別符号窃用型	検挙件数	502	785	576	398	482
	検挙事件数	155	216	190	182	215
セキュリティ・ホール攻撃型	検挙件数	18	2	9	10	9
	検挙事件数	6	2	9	8	8
計	検挙件数	520	787	585	408	491
	検挙事件数	160 (重複1)	218	199	189 (重複1)	223

※　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４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（104人）、次いで「14～19歳」（68人）、「30～39歳」（55人）の順となっている[注9]。

なお、令和４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62歳であった。

図３－１　令和４年に検挙した不正アクセス禁止法違反事件の年齢別被疑者数

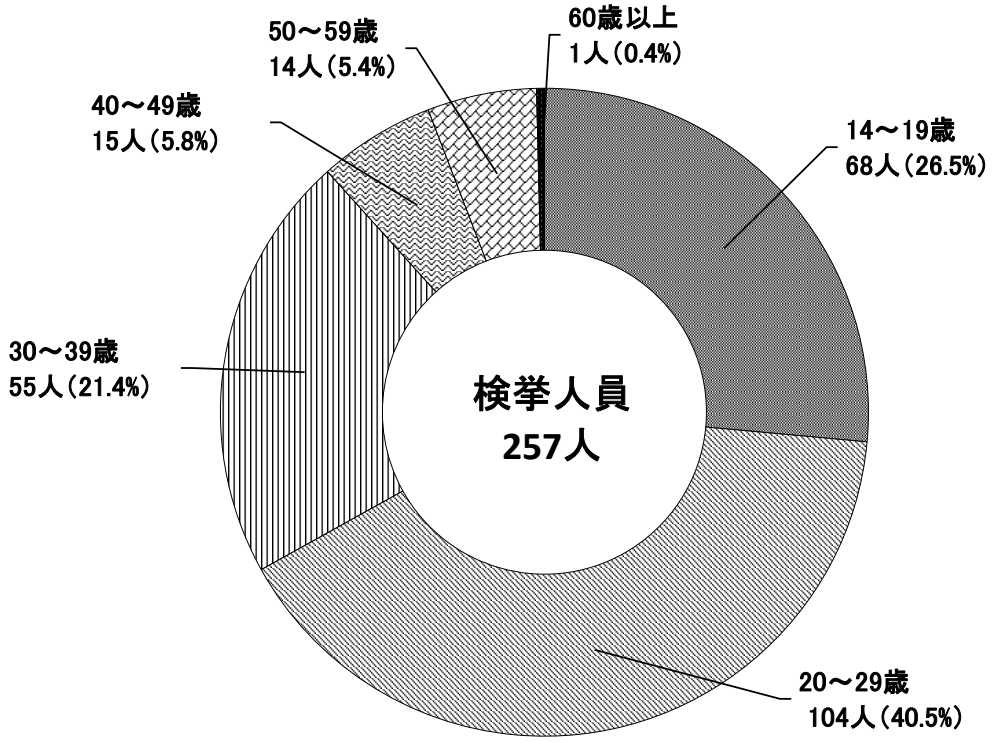


表３－１　年齢別被疑者数の推移（過去５年）

区分＼年次	平成30年	令和元年	令和2年	令和3年	令和4年
14～19歳	48	55	48	60	68
20～29歳	48	93	103	87	104
30～39歳	37	50	52	43	55
40～49歳	26	22	17	30	15
50～59歳	10	12	9	11	14
60歳以上	4	2	1	4	1
計	173	234	230	235	257

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６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４年に検挙した不正アクセス禁止法違反の検挙件数について、識別符号窃用型の不正アクセス行為の手口別に内訳を見ると、「利用権者のパスワードの設定・管理の甘さにつけ込んで入手」が最も多く（230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」（41件）の順となっており、前年（令和３年）と比べ、前者は約1.50倍、後者は約0.80倍となっている。

図３－２　令和４年における不正アクセス行為（識別符号窃用型）の手口別検挙件数

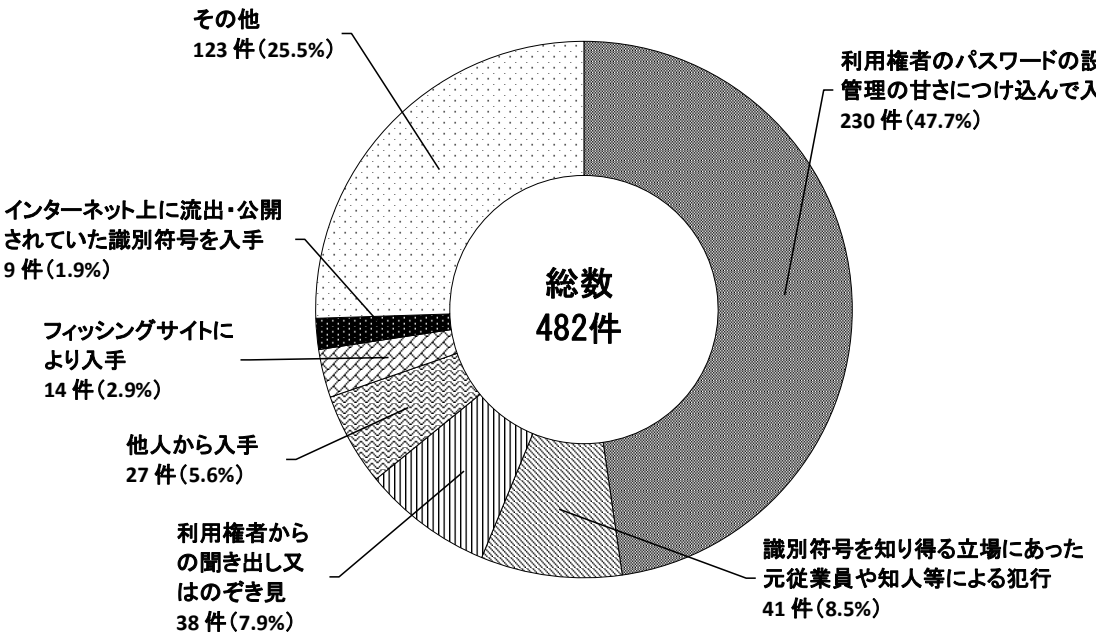


表３－２　不正アクセス行為の手口別検挙件数（過去５年）

区分＼年次	平成30年	令和元年	令和2年	令和3年	令和4年
識別符号窃用型	502	785	576	398	482
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	278	310	99	153	230
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	131	161	67	51	41
利用権者からの聞き出し又はのぞき見	17	20	115	36	38
他人から入手	13	182	78	34	27
フィッシングサイトにより入手	3	1	172	70	14
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	7	3	1	2	9
スパイウェア[注11]等のプログラムを使用して入手	0	5	3	0	0
その他	53	103	41	52	123
セキュリティ・ホール攻撃型	18	2	9	10	9

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４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（482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（233件）、次いで「社員・会員用等の専用サイト」（104件）の順となっており、前年（令和３年）と比べ、前者は約1.62倍、後者は約1.39倍となっている。

図３－３　令和４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

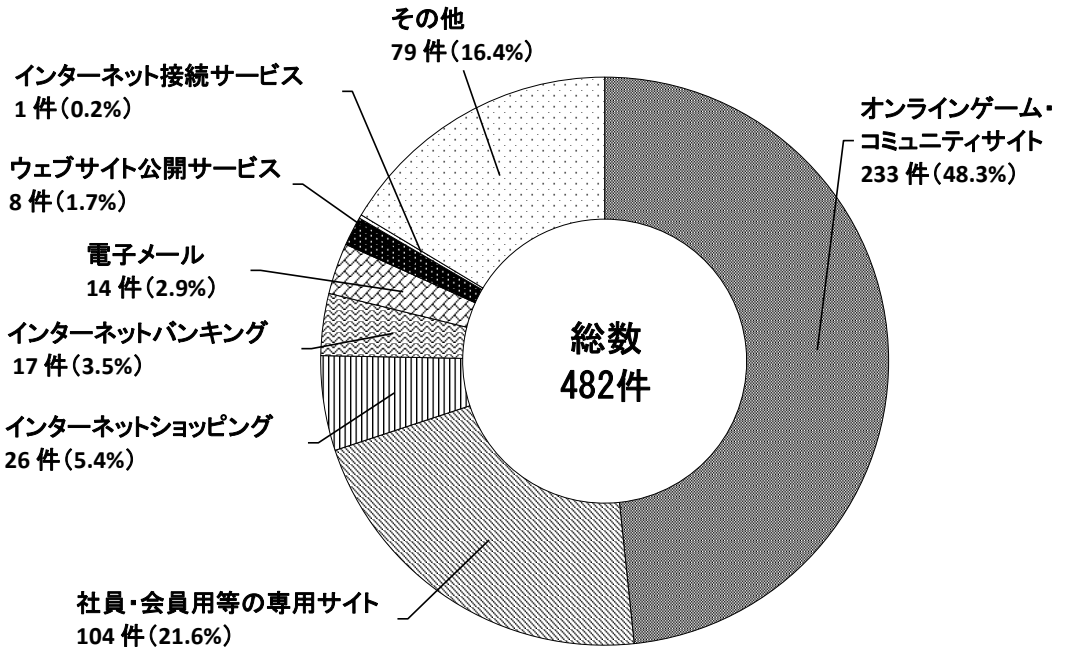


表３－３　不正アクセス行為（識別符号窃用型）により不正に利用されたサービス別検挙件数（過去５年）

区分＼年次	平成30年	令和元年	令和2年	令和3年	令和4年
オンラインゲーム・コミュニティサイト	217	224	88	144	233
社員・会員用等の専用サイト	200	151	174	75	104
インターネットショッピング	9	67	36	38	26
インターネットバンキング	7	14	12	96	17
電子メール	34	21	24	14	14
ウェブサイト公開サービス	3	5	1	4	8
インターネット接続サービス	9	5	1	0	1
インターネットオークション	6	4	1	0	0
その他	17	294	239	27	79
計	502	785	576	398	482

４　令和４年の主な検挙事例

(1)　無職の男（26）ほか３名は、共謀の上、令和３年９月、インターネット通販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ページをレンタルサーバに記録蔵置し、正規利用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４年２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。

(2)　飲食店従業員の男（49）は、令和３年12月から令和４年１月にかけて、元勤務先である法人が管理するＶＰＮ機器に不正アクセスした上で、同法人が管理するサーバに不正アクセスし、サーバ内のアクセス権限の設定を変更した。同年10月、男を不正アクセス禁止法違反（不正アクセス行為）及び私電磁的記録不正作出・同供用罪で検挙した。

(3)　地方公務員の女（34）は、令和２年５月から令和４年４月にかけて、同僚のＩＤ・パスワードを使用して勤務先のシステムに複数回不正アクセスし、自身の年次有給休暇の記録を削除するなどした。同年７月、女を不正アクセス禁止法違反（不正アクセス行為）及び公電磁的記録不正作出・同供用罪で検挙した。

(4)　無職の男（25）は、令和４年３月、他人のＩＤ・パスワードを利用してキャッシュレス決済サービス提供事業者が提供する決済サービスの認証サーバに不正アクセスし、正規利用者になりすまして不正に商品を購入した。同年４月、男を不正アクセス禁止法違反（不正アクセス行為）及び詐欺罪で検挙した。

(5)　会社員の男(45)は、令和４年６月から同年８月にかけて、面識のある女性のＩＤ・パスワードを使用してスマートフォン等の製造販売事業者が提供するオンラインサービスの認証サーバに不正アクセスし、同女のスマートフォンの位置情報を取得するなどした。同年12月、男を不正アクセス禁止法違反（不正アクセス行為）で検挙した。

(6)　自営業の男（41）は、令和３年10月、知人男性から通信販売事業者が提供するインターネットショッピングサイトで同男性が使用するアカウントのＩＤ・パスワードを言葉巧みに聞き出し、同男性のアカウントのパスワードを変更した上、変更後のパスワードを使用して同サイトに不正アクセスした。令和４年８月、男を不正アクセス禁止法違反（不正アクセス行為）及び私電磁的記録不正作出・同供用罪で検挙した。

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。

(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４年（令和４年１月１日から令和４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 226 件（令和３年：243 件）であった（注２）。令和４年は令和３年と比べて、17 件（約 7.0%）減少した。

届出の被害内容で主に見受けられたものは、令和３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、ウェブサイト（EC サイトを含む）の脆弱性を悪用した SQL インジェクション攻撃による情報窃取、そして業務委託先や利用サービスの提供元業者へのサイバー攻撃による情報窃取といったものであった。

次に、種々の切り口で分類した結果を示す。個々の件数には未遂（実際の被害はなかったもの）も含まれる。また、１つの届出について複数の項目に該当するものがあるため、それぞれの分類での総件数は届出件数に必ずしも一致しない。

(1) 手口別分類

届出を攻撃行為（手口）により分類したものである。総計は 655 件（令和３年：630 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 525 件（令和３年：457 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、ポートスキャンや脆弱性診断ツールを悪用したもの、アカウントの有効性確認を行うものなどであった。

(ｲ)　権限取得行為（侵入行為）

パスワード推測、システムの設定不備の悪用、またはソフトウェアのバグ等のいわゆる脆弱性を悪用した攻撃等により権限を不正に取得して侵入する行為である。

176 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：89 件

パスワード推測（パスワードリスト攻撃等）：54 件
システムの設定不備を悪用した攻撃：33 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。345 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込：107 件
資源利用(CPU 等のリソース不正使用)：44 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、７件（令和３年：２件）であった。

ウ その他
メール不正中継や正規ユーザになりすましてのサービスの不正利用、ソーシャルエンジニアリング等である。123 件（令和３年：171 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：83 件
ソーシャルエンジニアリング：８件
メール不正中継：１件

(2) 原因別分類
226 件の届出のうち、実際に被害に遭った 187 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 216 件（令和３年：220 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３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：83 件
原因不明：37 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）：34 件
ID、パスワード管理の不備：27 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：85 件
クライアント：57 件
メールサーバ：25 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 494 件（令和３年：367 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：94 件
不正プログラムの埋め込み：94 件
ファイルの書き換え：92 件

(5) 対策情報
冒頭で述べた通り、令和４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 216 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 38.4%（83 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 15.7%（34 件）であり、この２つの項目で約 54.1%（117 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 12.5%（27 件）を占める。

VPN 装置やウェブサイト等のサーバへの不正アクセスを防ぐためには、次のような対策を検討していただきたい。

システム管理者向け対策としては、

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

等、脆弱性を無くしていくことや、不正ログインを早急に検知できる機能の追加を検討することを勧める。

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/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/websitecheck.html

「安全なウェブサイトの作り方」
https://www.ipa.go.jp/security/vuln/websecurity.html

「JVN（Japan Vulnerability Notes）」 ※脆弱性対策情報ポータルサイト
https://jvn.jp/

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

【個人ユーザ向け】
「ここからセキュリティ」情報セキュリティ・ポータルサイト
https://www.ipa.go.jp/security/kokokara/
「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４年（令和４年１月１日から令和４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 58,389 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 41,173 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 7,872 件の報告があった。

[1/1-3/31: 1,174 件、4/1-6/30: 3,615 件、7/1-9/30: 1,917 件、10/1-12/31: 1,166 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 2,382 件の報告があった。

[1/1-3/31: 703 件、4/1-6/30: 557 件、7/1-9/30: 695 件、10/1-12/31: 427 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 851 件の報告があった。

[1/1-3/31: 291 件、4/1-6/30: 199 件、7/1-9/30: 199 件、10/1-12/31: 162 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 26 件の報告があった。

[1/1-3/31: 7 件、4/1-6/30: 7 件、7/1-9/30: 8 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 28,694 件の報告があった。
[1/1-3/31: 6,820 件、4/1-6/30: 8,088 件、7/1-9/30: 7,520 件、10/1-12/31: 6,266 件]

（６） 制御システム関連

インターネット経由で攻撃が可能な制御システム等については報告がなかった。
[1/1-3/31: 0 件、4/1-6/30: 0 件、7/1-9/30: 0 件、10/1-12/31: 0 件]

（７） 標的型攻撃

特定の組織、企業、業種などを標的として、マルウェア感染や情報の窃取などを試みる攻撃について 7 件の報告があった。
[1/1-3/31: 2 件、4/1-6/30: 2 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 1,341 件の報告があった。
[1/1-3/31: 372 件、4/1-6/30: 255 件、7/1-9/30: 315 件、10/1-12/31: 399 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]

2022 年 1 月	Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起(更新)
	2022 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（APSB22-01）に関する注意喚起(公開)
	2022 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)
	SonicWall SMA100 シリーズの複数の脆弱性に関する注意喚起(公開)
2022 年 2 月	2022 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)
	マルウェア Emotet の感染再拡大に関する注意喚起(公開)
	マルウェア Emotet の感染再拡大に関する注意喚起(更新)
	マルウェア Emotet の感染再拡大に関する注意喚起(更新)

2022 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）
	マルウェア Emotet の感染再拡大に関する注意喚起（更新）
	マルウェア Emotet の感染再拡大に関する注意喚起（更新）
	2022 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）
	Trend Micro Apex Central 製品の脆弱性（CVE-2022-26871）に関する注意喚起（公開）
2022 年 4 月	Apache Struts 2 の脆弱性（S2-062）に関する注意喚起（公開）
	2022 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（APSB22-16）に関する注意喚起（公開）
	2022 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）
	マルウェア Emotet の感染再拡大に関する注意喚起（更新）
	2022 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（更新）
	マルウェア Emotet の感染再拡大に関する注意喚起（更新）
2022 年 5 月	FUJITSU Network IPCOM の運用管理インタフェースの脆弱性に関する注意喚起（公開）
	2022 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）
	マルウェア Emotet の感染再拡大に関する注意喚起（更新）
	マルウェア Emotet の感染再拡大に関する注意喚起（更新）
	マルウェア Emotet の感染再拡大に関する注意喚起（更新）
2022 年 6 月	Confluence Server および Data Center の脆弱性（CVE-2022-26134）に関する注意喚起（公開）
	Confluence Server および Data Center の脆弱性（CVE-2022-26134）に関する注意喚起（更新）
	2022 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）
2022 年 7 月	2022 年 7 月マイクロソフトセキュリティ更新プログラムに関する注意喚起（公開）
	Adobe Acrobat および Reader の脆弱性（APSB22-32）に関する注意喚起（公開）
	2022 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）
2022 年 8 月	2022 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（APSB22-39）に関する注意喚起（公開）
	Movable Type の XMLRPC API の脆弱性に関する注意喚起（公開）
2022 年 9 月	Trend Micro Apex One および Trend Micro Apex One SaaS の脆弱性に関する注意喚起（公開）
	2022 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）
2022 年 10 月	bingo!CMS の認証回避の脆弱性（CVE-2022-42458）に関する注意喚起（公開）
	Fortinet 製 FortiOS、FortiProxy および FortiSwitchManager の認証バイパスの脆弱性（CVE-2022-40684）に関する注意喚起（公開）
	2022 年 10 月マイクロソフトセキュリティ更新プログラムに関する注意喚起（公開）
	Adobe Acrobat および Reader の脆弱性（APSB22-46）に関する注意喚起（公開）
	Fortinet 製 FortiOS、FortiProxy および FortiSwitchManager の認証バイパスの脆弱性（CVE-2022-40684）に関する注意喚起（更新）
	2022 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）
2022 年 11 月	OpenSSL の脆弱性（CVE-2022-3602、CVE-2022-3786）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）
	2022 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）

2022 年 12 月	FortiOS のヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）に関する注意喚起（公開）
	2022 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）
	Citrix ADC および Citrix Gateway の脆弱性（CVE-2022-27518）に関する注意喚起（公開）
	FortiOS のヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）に関する注意喚起（更新）
	FortiOS のヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）に関する注意喚起（更新）

（２）　活動概要（報告状況等の公表）

発行日：2022/1/20［2021 年 10 月 1 日～2021 年 12 月 31 日］
発行日：2022/4/14［2022 年 1 月 1 日～2022 年 3 月 31 日］
発行日：2022/7/14［2022 年 4 月 1 日～2022 年 6 月 30 日］
発行日：2022/10/20[2022 年 7 月 1 日～2022 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］421 件

注１　不正アクセス関連行為とは、コンピュータやネットワークのセキュリティを侵害する人為的な行為で、意図的（または、偶発的）に発生する全ての事象が対象になる。

注２　ここにあげた件数は、JPCERT/CC が受け付けた報告の件数である。実際のアタックの発生件数や、被害件数を類推できるような数値ではない。また類型ごとの実際の発生比率を示すものでもない。一定以上の期間に渡るアクセスの要約レポートも含まれるため、アクセスの回数と報告件数も一般に対応しない。報告元には、国内外のサイトが含まれる。

注３　「インシデント件数」は、各報告に含まれるインシデント件数の合計を示す。ただし、1 つのインシデントに関して複数件の報告がよせられた場合は、1 件のインシデントとして扱う。

アクセス制御機能に関する技術の研究開発の状況

１　国で実施しているもの

総務省又は経済産業省が取り組むアクセス制御機能の研究開発に関してとりまとめたものであり、具体的には、独立行政法人自ら又は委託による研究、国からの委託又は補助による研究である。

実施テーマは以下の７件であり、その研究開発の概要は、別添１のとおりである。

- サイバーセキュリティ技術の研究開発
- Web媒介型攻撃対策技術の実用化に向けた研究開発
- 欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発
- サイバー攻撃ハイブリッド分析実現に向けたセキュリティ情報自動分析基盤技術の研究開発
- 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４年12月５日から令和５年１月20日までの間にアクセス制御機能に関する技術の研究開発状況の募集を行ったところ、次のとおり４社から計４件の提案があった。それぞれの研究開発の概要は、別添２のとおりである。

なお、別添２の内容は当該企業から応募のあった内容を原則としてそのまま掲載している。

- 株式会社SYNCHRO
- 株式会社スプライン・ネットワーク
- かっこ株式会社
- アドソル日進株式会社

(2)　調査

警察庁が令和４年９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、９件）

福岡大学（２件）
明星大学
関東学院大学
名古屋大学
東北工業大学
玉川大学
岩手大学

日本文理大学

イ　企業（３社、10件）

株式会社テリロジーワークス

ルネサスエレクトロニクス株式会社（２件）

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３のとおりである。

なお、別添３の内容は、アンケート調査の回答内容を原則としてそのまま掲載している。

アンケート調査は、以下の条件に該当する大学及び企業の中から、調査対象として無作為抽出した大学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　インシデント分析技術
テーマ名　サイバーセキュリティ技術の研究開発
開発年度　平成18年度～
実施主体　国立研究開発法人情報通信研究機構 **法人番号**　7012405000492
背景、目的 サイバー攻撃の急増と被害の深刻化によりサイバーセキュリティ技術の高度化が不可欠となっていることから、ネットワークを介したサイバー攻撃やマルウェア等の活動を大局的に把握・対応するための各種観測技術、分析技術、可視化等の研究開発を行う。
研究開発状況（概要） これまでに研究開発・整備したサイバー攻撃観測機構や、マルウェアの収集・分析機構に関して、世界規模の観測網確立に向けた観測規模の更なる拡充、より高度な観測・分析機構の開発等を行った。観測・分析結果については、Webサイト等で広く公開するとともに、アラートシステム等の外部への技術移転を行った。また、地方自治体へのアラート提供を拡大する等、研究開発成果の社会展開を推進した。
詳細の入手方法（関連部署名及びその連絡先） 国立研究開発法人情報通信研究機構　サイバーセキュリティ研究所　サイバーセキュリティ研究室　042-327-6225
将来の方向性 上記の研究開発を通じて、将来のネットワーク自身及びネットワーク上を流通する情報の安全性・信頼性の確保と、利用者にとって安全・安心な情報通信基盤の実現を目指す。

対象技術　インシデント分析技術

テーマ名　Web媒介型攻撃対策技術の実用化に向けた研究開発

開発年度　平成28年度～令和2年度

実施主体　株式会社KDDI総合研究所、国立大学法人横浜国立大学他（国立研究開発法人情報通信研究機構が実施する委託研究の委託先）
法人番号　5030001055903（KDDI総合研究所）、6020005004971（横浜国立大学）

背景、目的

Webを媒体としたサイバー攻撃は拡大の一途を辿っており、情報処理推進機構（IPA）が公表している「情報セキュリティ 10大脅威2015」においても、Web系の脅威が約半数を占め、国民の関心は高い。平成27年6月に公表された日本年金機構からの年金情報流出においては、不正なWebサイトへの誘導も行われたと報道されており、Web系の脅威とその対策は依然、重要課題である。

また、従来からあるWebの改ざんや「ドライブ・バイ・ダウンロード攻撃」に加え、標的型攻撃にWebサーバを利用する「水飲み場攻撃（watering hole attack）」や、オンラインバンキングユーザを狙ってWebブラウザ経由で情報を窃取する「バンキングマルウェア」、検索エンジン経由で不正なWebサイトに誘導する「SEO（Search Engine Optimization）ポイゾニング」など、攻撃手法が多様化・複雑化してきている。さらに、攻撃対象がWindows OSのみならず、Mac OSやAndroid等のモバイル端末、IoT機器（linux組込み系機器）にまで広がってきており、重大な社会問題となっている。

そこで、これまで機構が委託研究として取り組んできた「ドライブ・バイ・ダウンロード攻撃対策フレームワークの研究開発」（平成24年度～平成27年度）を実用化に向けてさらに発展させ、観測対象をWindows OSのみならず、Mac OSやモバイル端末、IoT機器等に拡大するとともに、Webを媒体とした新たなサイバー攻撃への抜本的な対策に資する観測・分析・対策技術を確立する。

研究開発状況（概要）

平成28年度から以下の研究開発を開始。平成30年度に行った中間評価の結果、令和2年度までの延長を決定。

（１）新型ブラウザセンサの研究開発
（２）新型観測機構の研究開発
（３）新型攻撃情報分析基盤の研究開発
（４）Web媒介型攻撃対策技術大規模・長期実証実験

詳細の入手方法（関連部署名及びその連絡先）

国立研究開発法人情報通信研究機構 イノベーション推進部門 委託研究推進室
（https://www.nict.go.jp/collabo/commission/k_190.html）
電話 042－327－6011

将来の方向性

上記セキュリティ対策技術を確立し、高度情報通信ネットワーク社会の安全性・信頼性の確保に資する。

対象技術　侵入検知・防御技術、ぜい弱性対策技術

テーマ名　欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発

開発年度　平成30年度～令和3年度

実施主体　東日本電信電話株式会社、学校法人慶應義塾他（国立研究開発法人情報通信研究機構が実施する委託研究の委託先）

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

背景、目的

本研究開発は、欧州との連携により研究開発の促進が期待できる領域について、欧州委員会（EC: European Commission）と連携して共同で実施するプログラム。

ハイパーコネクテッド社会の実現に向けて、実践的なサイバーセキュリティ技術の研究開発は不可欠である。そのため、セキュリティ、IoT、クラウド及びビッグデータを組み合わせた先端技術の研究開発及び実証を通じ、世界規模で有効かつ実効性のあるサイバーセキュリティ基盤技術の構築を目指す。

研究開発状況（概要）

平成30年度から研究開発を開始。

具体的には、「新たな脅威への機敏な対応」、「脆弱性自動検出/自動修復」、「セキュリティツールのオープンソース化」、「IoTセキュリティ」、「クラウドセキュリティ」、「データセキュリティ」、「プライバシー保護」、「データ匿名化」、「IoT／クラウドに関するブロックチェーン」、「重要インフラ保護」、「クロスボーダ・アプリケーション」に関わる研究開発及び実証を行う。

詳細の入手方法（関連部署名及びその連絡先）

国立研究開発法人情報通信研究機構 イノベーション推進部門 委託研究推進室
（https://www.nict.go.jp/collabo/commission/k_195.html）
電話 042－327－6011

将来の方向性

国際標準化を睨んだ研究開発力の強化や国際実証環境の構築を軸とした共同研究開発に取り組むことにより、情報通信基盤の共通化を通じた豊かな社会への貢献に資する。

対象技術　インシデント分析技術

テーマ名　サイバー攻撃ハイブリッド分析実現に向けたセキュリティ情報自動分析基盤技術の研究開発

開発年度　令和元年度～令和2年度

実施主体　国立大学法人九州大学、学校法人早稲田大学 他（国立研究開発法人情報通信研究機構が実施する委託研究の委託先）
法人番号　3290005003743（国立大学法人九州大学）、5011105000953（学校法人早稲田大学）他

背景、目的

マルウェアへの感染は世界的な問題であり、政府、重要インフラなどの組織に対する脅威は増加の一途を辿っている状況であるが、感染活動の早期把握やそのマルウェアに関する情報の関連組織間での共有ができていない。

この問題の解決には、セキュリティインシデント発生の可能性をより早く検知し、それを分析するための関連情報を自動的に生成し、関連付け、そのインシデントのもととなったマルウェアや脆弱性を分析する必要がある。これらのタスクは大量のデータを分析することが求められるため、人手による分析は非現実的である一方で、コンピュータによる自動処理の効果が大きく期待できる領域である。また、これらの分析は単一の分析にて完結するものではなく、例えばライブネットトラフィック分析やダークネットトラフィック分析、マルウェア分析、脆弱性分析、Web情報分析など、様々な分析結果を総合的に判断するハイブリッド分析が求められる。そこで本研究では、国立研究開発法人情報通信研究機構が開発中のマルウェア活動の活性化を自動的に検知する技術と連携し、その検知したイベントに関連するマルウェア・脆弱性・脅威情報などを実時間で精緻に提供することで、より有用性の高いセキュリティ情報自動分析基盤技術の確立を目指す。

研究開発状況（概要）

令和元年度から以下の研究開発を開始。

（1）サイバー攻撃インフラ情報の収集と分析、（2）実時間で実現可能な大規模かつ構造的なマルウェア分析、（3）インテリジェンス情報の生成と分析について

詳細の入手方法（関連部署名及びその連絡先）

国立研究開発法人情報通信研究機構 イノベーション推進部門 委託研究推進室
（https://www.nict.go.jp/collabo/commission/k_21601.html）
電話 042－327－6011

将来の方向性

感染活動を自動的に検知し、マルウェアに関する情報と共に自動的に警告を提供可能となる。安心・安全な国際的なサイバー社会の構築・運営に大きく貢献する。

対象技術	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（予定）
実施主体 **法人番号**	ジャパンデータコム株式会社、学校法人早稲田大学 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６年度（予定）
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、高い安全性と効率性（速度、メモリ等）を両立する暗号技術の研究開発を行う。
研究開発状況（概要） 複雑なアクセス制御を柔軟に実現する高機能暗号技術や、暗号化した状態で検索や計算を行う秘密計算技術（秘匿データベースについては企業との連携で実用化事例あり）、匿名認証技術、さらにはIoT機器との通信のセキュリティを高める軽量暗号技術等の提案を行っている。
詳細の入手方法（関連部署名及びその連絡先） 国立研究開発法人 産業技術総合研究所 サイバーフィジカルセキュリティ研究センター TEL: 03-3599-8001（代表） URL:https://www.cpsec.aist.go.jp/
将来の方向性 データの授受に関わるハードウェア、ソフトウェアのセキュリティ対策技術と組み合わせることで、サイバーフィジカルシステム全体のセキュリティ測定、強化、保証する技術を確立していく。

（別添２）

企業名（及び略称）　株式会社SYNCHRO 法人番号　1010001126544	
代表者氏名　室木 勝行	
所在地（郵便番号及び住所）〒102-0073 東京都千代田区九段北1-10-9 九段VIGAS 5階	
関連部署名及び電話番号　サイバーセキュリティー対策センター ken@udc-synchro.co.jp, 083-902-2518	
ＵＲＬ　https://www.udc-synchro.co.jp/	
対象技術	技術開発状況
その他アクセス制御機能に関する技術 令和2年	暗号鍵とIPv6アドレスに関連を持たせることで中間者攻撃、なりすまし原理的に排除する機能を持つオープンソースソフトウェア（Yggdrasil, Cjdns）とip[46]tablesなどOSの機能を利用し、既存のIPネットワーク上で仮想閉域網の構築とEnd-to-Endでの暗号化、デバイス認証を行うミドルウェアを開発しました。 上記技術を、ビジネスチャットシステム、Web会議システム、IPv4トンネリング用デバイス、セキュアECサイト、IPカメラ、IP-PBXなどに応用し、令和3年から、ソフトウェアプロダクト、あるいは、アプライアンス製品としての販売を開始しています。 また、上記技術は、山口県の「デジテックオープンイノベーション」で採択された「高齢者の生活利便性向上にむけた支援サービスの構築」にも適用されています。

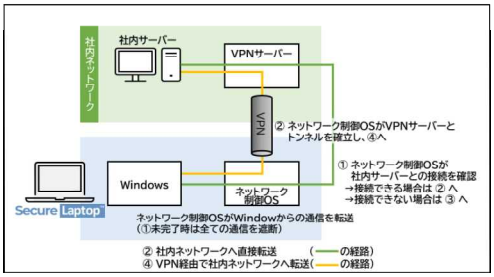
企業名（及び略称） 株式会社スプライン・ネットワーク 法人番号 4011001040914	
代表者氏名 雪野　洋一	
所在地（郵便番号及び住所） 〒150-0034東京都渋谷区代官山町1-8 SYLA DAIKANYAMA 6F	
関連部署名及び電話番号 WiSAS事業部　03-5464-5468	
ＵＲＬ https://www.spline-network.co.jp/	
対象技術	技術開発状況
① 侵入検知・防御技術 ② ぜい弱性対策技術 市場展開： 令和2年1月～	Wi-Fi領域のセキュリティを強化したいエリアに、独自開発のセンサーを設置し、弊社のクラウドセンターからリモートで管理するフルマネージド型のWi-Fiセキュリティ常時監視システムを開発。 センサーがWi-Fi電波を常時監視し、可視化や分析を行うことでWi-Fi環境における不正利用やサイバー攻撃による情報漏洩を防止。 ・非認可端末　・なりすましAP　・Mac偽装　・Wi-Fi Direct ・ハッキングツール　・シャドーIT　・野良デバイスなどを検出／遮断 ※この技術を核に日本初の統合Wi-Fiセキュリティ・ソリューションを提供中 ・製品名：Wi-Fi Security Assurance Series　略称：WiSAS) ・詳細： https://wisas.jp（日本国内特許取得済み、PCT国際特許出願中）

企業名（及び略称） 法人番号	かっこ株式会社 9010001137889
代表者氏名	代表取締役社CEO 岩井裕之
所在地（郵便番号及び住所）	東京都港区元赤坂1-5-31新井ビル4F
関連部署名及び電話番号	O-MOTION事業部　03-6447-4535
ＵＲＬ	https://cacco.co.jp/
対象技術	技術開発状況　2016年より「O-MOTION」としてサービス提供開始
その他アクセス制御機能に関する技術 開発年： 平成28年	・端末特定技術 100項目以上のパラメータを用い、高精度に端末の特定ができます。他ツールでは単一のパラメータで端末を特定しますが、当社サービス「O-MOTION」で活用している「端末特定技術」では、複数要素を用いた判断が可能です。そのため、端末情報の１つであるIPアドレスなど情報を意図的に変えてくる不正を見逃しません。 ・キータッチなどの操作情報の活用 端末のタイピング方法やマウスの動きを元に、ユーザーが意識することなく不正アクセスの審査が行えるため、サービスの使い勝手に影響を与えません。botのような人間の挙動と異なるケースも把握することができ、不正者にとって挙動を偽造することが困難なため不正検知にとって有効です。 上記2点の技術をかけ合わせ、正しいID・パスワードによるアクセスであっても、そのアクセスが本当に本人によるものであるのか、不正者による不正アクセスなのかを判断するクラウドサービスとして、通販サイト、金融サービスサイト（インターネットバンキング・ネット証券）、会員サイト等に「O-MOTION」として提供しています。

<table>
<tr><td colspan="2">企業名（及び略称）アドソル日進株式会社
法人番号　8010401052268</td></tr>
<tr><td colspan="2">代表者氏名　　山中　直道　（セキュリティ・ソリューション事業部）</td></tr>
<tr><td colspan="2">所在地（郵便番号及び住所）〒108-0075 東京都港区港南４丁目１番８号</td></tr>
<tr><td colspan="2">関連部署名及び電話番号　セキュリティ・ソリュ―ション事業部　03-5796-3260</td></tr>
<tr><td colspan="2">ＵＲＬ　https://www.adniss.jp/</td></tr>
<tr><td>対象技術</td><td>技術開発状況</td></tr>
<tr><td>・その他アクセス制御機能に関する技術

開発年：
令和３年</td><td>ネットワークに接続された端末デバイスは、様々な不正アクセス行為に晒されている。以下に示すアクセス制御機能を開発することで、電子計算機に係る犯罪の防止及不正アクセス行為が行われにくい環境を実現。

【環境構築例１】
1台の端末内で複数のシステム、複数ネットワークを完全隔離した環境を確立（異なるセキュリティポリシーのネットワークを完全分離した状態で運用可能）。
例えば、機密情報がある業務システムのネットワークとインターネットを完全に切り離し、外部からサイバー攻撃を受けても業務システムのネットワーク環境に侵入させず、情報漏洩を防止。
 

【環境構築例２】
社外から、社内ネットワークなどの信頼できるネットワークに接続する場合、安全なネットワークが確立されるまでの間、Windowsをネットワークに接続させず、外部からの不正アクセス等の脅威からデータを隔離し、情報漏洩を防ぐ技術を開発。
 

安全なVPN接続が完了するまでは全てのWindows通信を遮断、Windows通信は常に安全な経路が確立された事を確認し、適切なネットワークに自動接続を行う技術特徴を持つ。
この技術特徴を生かし、家庭や公衆ネットワークから安全に社内ネットワークに接続し、セキュアなテレワークを実現など、不正アクセスが行われにくい環境が構築できる。

■環境名：セキュア・アイソレーション
https://www.adniss.jp/products/products-detailed/secure-isolation.html
■環境名：セキュア・ラップトップ
https://www.adniss.jp/products/products-detailed/secure-laptop.html</td></tr>
</table>

（別添３）

ア　大学

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： 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は以下のとおり。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～2023年3月31日	現段階では少数の被験者の協力による認証精度を確認している。極めて高い認証精度を確認しており、近日中に多くの被験者を用いて、認証精度を検証する計画である。現在は、国内のセキュリティ製品を開発するメーカーと共同研究開発を推進することを協議しており、同メーカーから日本国内に向けて販売することを目指す。

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

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	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　末田研究室
ホームページのURL	https://www.meisei-u.ac.jp
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： IoTデバイスにおけるセキュリティソフト導入の検討 研究開発国： 日本 研究開発時期： 2022年4月～2023年3月	IoT機器は数や種類、使用用途が豊富であることや、スペック等の問題からアンチウイルスソフトの導入が困難とされており、ユーザ側で有効な対策が実施できないとされている。こうしたことを背景に、近年のCPU、メモリ等の軽量化が進んでいることに着目しIoT機器のスペックを考慮したアンチウィルスソフトの調査および導入を検討し、問題点についても明らかにする。現在、アンチウィルスソフトの調査を実施中である。

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	関東学院大学理工学部
代表者名	理工学部長　辻森淳
所在地	〒236-8501 神奈川県横浜市金沢区六浦東1-50-1
窓口部署名	学部庶務課（理工学部、建築・環境学部）
電話番号	045-786-7096
関連部門名	理工学部ネットワークセキュリティ研究室
ホームページのURL	https://univ.kanto-gakuin.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： ブロックチェーン上での安全な鍵管理方式の研究 研究開発国： 日本 研究開発時期： 2018年～2022年	ブロックチェーンの性質を損なうことなく秘匿化した情報を利活用するために、秘密分散などの手法を応用することで、ブロックチェーン上で安全に秘密鍵を運用する方式を提案した[1]。[1]吉田祥悟、塚田恭章：ブロックチェーン上での安全な鍵管理方式と単一障害点のない秘密計算方式の提案.情報処理学会論文誌（採録決定）

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	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	大学院情報学研究科　高田・松原研究室/組込みシステム研究センター
ホームページのURL	
研究説明のURL	https://www.ertl.jp https://www.nces.i.nagoya-u.ac.jp
対象技術	技術の概要・特徴など
研究開発名称： 組込みシステム向けのセキュリティ技術 研究開発国： 日本 研究開発時期： 2014年4月1日	大学の研究組織にて、組込みシステムや自動車制御システムを対象に、次のようなセキュリティ技術について研究・開発を進めている。なお、これらの活動は、研究室独自、または企業との共同研究として実施している。開発した成果の一部は、学術論文として発表している。 ・脅威、脆弱性分析技術・ソフトウェアの実行フロー保証技術・ソフトウェア更新の支援技術・ソフトウェアに対するファジングによるテスト技術・制御ネットワークへの不正アクセス防止技術・制御ネットワークにおけるメッセージ認証技術　上記に関連して、組込み・自動車セキュリティに関する社会人向け教育活動を、名古屋大学NCES人材育成プログラムとして提供している。 https://www.nces.i.nagoya-u.ac.jp/NEP/index.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	学校法人東北工業大学
代表者名	
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～	要素技術の検討と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	学校法人玉川学園
代表者名	小原芳明
所在地	〒194-8610 東京都町田市玉川学園6-1-1
窓口部署名	玉川大学　学術研究所　研究推進室
電話番号	042-739-8666
関連部門名	量子情報科学研究所
ホームページのURL	https://www.tamagawa.jp
研究説明のURL	https://www.tamagawa.jp/research/quantum/qec.
対象技術	技術の概要・特徴など
研究開発名称： 光通信量子暗号（Y00） 研究開発国： 日本 研究開発時期： 2011年4月1日～	光通信量子暗号Y-00は光が本質的に持つ量子力学的な雑音の効果を活用してデータを秘匿する機能を実現する、光通信回線を守る技術です。この機能を実証するためのプロトタイプをすでに公開しており、引き続き大学の研究機関としてその基礎的解明・発展に向けて実験研究と理論研究の両面から研究を推進しています。最新の研究成果は論文として発表しているのでそちらを参照されたい。

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

企業・大学名	国立大学法人岩手大学
代表者名	学長　小川智
所在地	〒020-8550 岩手県盛岡市上田3-18-8
窓口部署名	理工学部事務部
電話番号	019-621-6305
関連部門名	理工学部システム創成工学科知能・メディア情報コース
ホームページのURL	https://www/iwate-u.ac.jp/
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： マルウェアの検出・分類に関する研究 研究開発国： 日本 研究開発時期： 2016年4月～	マルウェアの表層あるいは動的解析結果を利用した機械学習による検出・分類手法の研究を行っている。

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

企業・大学名	日本文理大学
代表者名	学長　橋本堅次郎
所在地	〒870-0397 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	工学部・情報メディア学科
ホームページのURL	www.nbu.ac.jp
研究説明のURL	https://www.nbu.ac.jp/～fukushima https://sites.google.com/view/fukulab
対象技術	技術の概要・特徴など
研究開発名称： 生体情報の継続認証による時間追従型本人認証システム 研究開発国： 日本 研究開発時期： 2000年9月～	通信回線が低遅延化が進むとともに、新型コロナに伴うニーズの多様化等の社会的変化があることから、ニーズの変化に伴う設計と、確定した設計から実装による社会実装の可能性検証、の2つを並走しての開発を進めている。　【ニーズ分析と設計（基礎理論/アルゴリズム）】・時間追従アルゴリズム　短時間推定および推定精度評価アルゴリズム　・特徴量記述　音声の特徴量化（頭部構造に着目したうめき声も対象とした取組）環境音の特徴量化（使用端末検知の次を見越した取組）【社会実装に向けた可能性検証】確定アルゴリズムの適用先としていくつかの企業と協力して試作・評価に向けた取り組みを進めている。

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	

イ　企業

企業・大学名	（株）テリロジーワークス
代表者名	
所在地	〒102-0073 千代田区九段北1-10-1
窓口部署名	ビズネス開発部
電話番号	03-5213-5533
ホームページのURL	www.twx-threetintel.com
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： THX 開発元(メーカー名等)： （株）テリロジーワークス 開発国： 日本 価格：300万～ 発売時期： 2021年10月 出荷数：	ネットワークトラフィックから得られるメタデータ情報を集収し解析プラットフォームに提供します。

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	ルネサスエレクトロニクス株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	https://www.renesas.com
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： 　セキュリティ対応マイコン 開発元(メーカー名等)： 　ルネサスエレクトロニクス株式会社 開発国： 　日本 価格： 発売時期： 出荷数： 	セキュリティ対応マイコンは、外部からのアクセス不可能なSecureIPを搭載します。SecureIP内にて鍵データと暗号エンジンを強固に保護し、領域保護機能や製品固有の機能と組み合わせることで、認証プログラムを改ざんの脅威から保護します。これにより、Root of Trustによる自立したセキュリティを実現し、様々な脅威から簡単かつ強固に保護するシステムを構築することが可能となります。

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

企業・大学名	ルネサスエレクトロニクス株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	ルネサスエレクトロニクス株式会社　セキュリティコンピテンスセンター
ホームページのURL	https://www.renesas.com
研究説明のURL	https://www.renesas.com/rx-security-solution
対象技術	技術の概要・特徴など
研究開発名称： SecureIP開発 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	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： 	IoT機器への攻撃動向を観察するためのハニーポット 販売目的での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	
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。出展 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： 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・処理機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,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。出展 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	
関連部門名	情報記述総合研究所
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年頃	「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が同じ平分であった場合、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/coeporate/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頃	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頃	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ュミレータを開発。

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	○