NICT NEWS
国立研究開発法人
情報通信研究機構
No.1
2025
通巻509

20th Anniversary
NICT創立20周年

FEATURE

広大なネットで戦う サイバーセキュリティ特集

対談

VRアーティスト
せきぐち あいみ さん

×

NICTサイバーセキュリティ研究所　研究所長
井上 大介

VRアーティストと語る脳のセキュリティ
脳は究極の個人情報だ

CONTENTS

NICT NEWS 2025 No.1 通巻509
国立研究開発法人情報通信研究機構

表紙画像：
Web媒介型サイバー攻撃の実態把握と対策技術向上のためのユーザー参加型プロジェクト「WarpDrive」。『攻殻機動隊 SAC_2045』とのタイアップにより、同作品に登場するキャラクター「タチコマ」をモチーフとしたソフトウェア「タチコマ・セキュリティ・エージェント」を開発。

左上画像：
Androidスマートフォン向けに無償配布しているアプリ「タチコマ・セキュリティ・エージェント・モバイル」。画像は『攻殻機動隊 SAC_2045』シリーズの世界に没入し、遊びながら現実社会のセキュリティやITの知識を学べるゲーム機能の一画面。

研究紹介ムービー『NICTステーション』(第2弾)が完成!

2024年12月、NICTの研究成果を理解していただくためのムービー『NICTステーション』(第2弾)が完成しました。

NICTを訪れたレポーターに、研究者と公式キャラクター“N”が以下の6つのテーマに関して、その研究内容と社会的インパクトをわかりやすく楽しく説明します。

リモートセンシング技術、電磁環境技術、レジリエントICT、WarpDrive、音声マルチスポット再生技術、分子モーター

ナレーションは『NICTステーション』(第1弾)と同様、**上白石萌音**さん。
未来が待ち遠しくなるムービーを是非ご覧ください。

https://www2.nict.go.jp/publicity/nict_station

2025年 年頭のご挨拶

明けましておめでとうございます。

国立研究開発法人情報通信研究機構
理事長 徳田 英幸

2025年の新春を迎えるにあたり、謹んで新年の挨拶を申し上げます。

皆様方には、日頃より、情報通信研究機構（NICT）に対して格別なご理解とご協力を賜り心よりお礼を申し上げます。

昨年は、１月に能登半島地震、９月に能登半島豪雨など自然災害が特定地域に重なり、被災地の復旧、復興の難しさを痛感したとともに、情報インフラの強靭化の重要性を改めて認識しました。また、４月には、NICTが通信総合研究所（CRL）と通信・放送機構（TAO）の合併により誕生し、20年を迎えました。この20年の間、産学官をはじめ関係者の皆様、さらに歴代の役職員の皆様に、様々な形でご支援を賜り、現在の姿にまで到達できたこと、重ねて感謝申し上げます。

さて、今年2025年４月からは、第5期中長期計画（5年間）の最終年度を迎えます。

第5期中長期計画では、重点的に研究開発を行う５つの分野として、電磁波先進技術分野、革新的ネットワーク分野、サイバーセキュリティ分野、ユニバーサルコミュニケーション分野、フロンティアサイエンス分野の研究開発を進め、また、政府戦略を踏まえ、Society 5.0の早期実現に向けた次世代ICT基盤に必要不可欠な先端技術として、戦略的に推進すべき研究4領域（Beyond 5G、AI、量子情報通信、サイバーセキュリティ）についても積極的に研究開発を進めてきました。特に、AI分野においては、生成AIの利用が社会に浸透し、様々な社会的な課題も顕在化しつつあります。NICTでは、日本政府が提案し、設置が承認されたGPAI(Global Partnership on AI)東京専門家支援センターを昨年７月に開設するとともに、AI関連の研究開発を加速するためのAI研究開発推進ユニットを9月に設置しました。さらに、サイバーセキュリティに関しても、NICT法を改正して、新しいNOTICE事業の推進、また従来の研究機関としての枠に留まらず、大学、民間企業も含めた我が国全体の研究開発を推進するハブとなるべくCYNEXアライアンスの活動を強化してきました。

その中でも、Beyond 5G領域では、非地上系ネットワーク（NTN）、時空間同期技術、テラヘルツ通信技術での研究開発に加え、国際共同研究プロジェクトや国際標準化活動にも積極的に参加し、成果をあげてきています。今年3月には、バルセロナで開催されるMWC25（Mobile World Congress 2025）において、その成果を広く世界に発表する予定です。

AI領域では、グローバルコミュニケーション計画2025を基に、VoiceTraを通じて長年利用されてきた多言語翻訳技術を同時通訳レベルまでに進化させることに成功しました。この技術は、今年4月から開催される大阪・関西万博において広く利用いただけるようになります。さらに今後発展が期待される大規模言語モデル（LLM）においても、WISDOM-Xなどのこれまでの成果と大規模日本語データセットを基に、日本語を中心とした生成AIの研究開発を加速しています。

量子ICT領域では、この５年の中で、量子ICT協創センターを発足させ、我が国の量子セキュリティ技術の研究拠点として、研究開発、テストベッド、社会展開、人材育成という4つの機能を軸として、新たな融合領域の開拓を先導しています。特に、人材育成プログラム のNQC（NICT Quantum Camp）や若手チャレンジラボが根付いてきています。

サイバーセキュリティ領域では、20年以上弛まず続けてきたサイバーセキュリティの技術・ノウハウを新たに発足させたサイバーセキュリティネクサスにおいて、サイバーセキュリティ情報とサイバーセキュリティ人材を育成する共通基盤を広く国内の産官学に展開し、日本のサイバーセキュリティ対応能力向上を目指しています。さらに、セキュリティ分野へのAI技術の応用だけでなく、AIシステムのセキュリティに関しても積極的に研究を推進しています。

また、NICTの重要な業務の１つである、公的サービスに関しても、日本標準時、無線機器の校正、CYDERなどのサイバートレーニングプログラム、宇宙天気予報業務を着実に実施していきます。宇宙天気予報業務では、今年が、太陽活動の11年周期の極大期を迎えることから、既に昨年から大規模な太陽フレア活動発生ごとに国民の皆様に注意を呼びかけておりますが、今年は引き続き緊張感をもって、本サービスの提供にあたる所存です。

皆様におかれましては、NICTが目指す「知の限界を超え、未来の社会基盤を創る」に向けた取組に対して、更なるご支援とご協力を賜りますことをお願い申し上げます。

結びに、皆様の益々のご健勝とご発展を祈念いたしまして、年頭の挨拶とさせていただきます。

VRアーティストと語る脳のセキュリティ 脳は究極の個人情報だ

空間に立体を描く世界的VRアーティスト・せきぐちあいみさん。最先端テクノロジーとアートの融合は、これまで見たことのない新鮮な造形を見せてくれる。そこはサイバー空間の「リアル」であり、身体の限界を超えた近未来のメタバースだ。

しかし、「光」とともに「闇」もある。アートもリアルの生活もすべてが仮想化されていくこの時代に、私たちはどのように適応していけばいいのだろうか。対話は、「創造する脳」から「脳のセキュリティ」にまで進んでいく。

井上　せきぐちさんは、最先端のバーチャルテクノロジーを活用して空間に3Dアートを描き出すVRアーティストとして、世界中から注目を集めています。どのようなきっかけで始められたのですか。

せきぐち　VRでは、何もない空間に仮想的に立体の造形が生みだせるのが、まるで魔法のようで感動したのが始まりです。

井上　現在は、世界で活躍していらっしゃるのですね。

せきぐち　はい、日本のほか、アメリカ、ドイツ、フランス、UAEのドバイなどでVRパフォーマンスを演じています。VRゴーグルを装着して空間にリアルタイムで描かれる造形に感動していただいております。海外のデジタルテクノロジー関係の展示会からもお声がかかり、このあいだはアフリカのモロッコで開催されたアフリカ最大の展示会に行ってきました。そこでも、海外の若者たちが私のアートに、すごく興味をもってくれました。

井上さんの研究所はどのような研究をされているのですか。

井上　私の研究所は、サイバー空間で行われている悪意のある攻撃から大切な情報やシステムを守る技術の研究・開発を行っています。

具体的には、サイバー攻撃をいち早く察知して攻撃を遮断したり無害化したりする技術の開発、サイバー空間を流れる情報を守る暗号の研究、攻撃手法の研究やマルウェアの解析などを行っています。サイバー攻撃の察知に関しては、ネットワーク内のどこが攻撃を受けているかが一目で分かるように可視化したことが大きな特長です。可視化することで攻撃をいち早く検知できますし、攻撃の内容・被害の詳細なども簡単な操作で知ることができます。この可視化されたシステムを社会展開することによって、熟練していないシステム管理者や経験の少ない若いエンジニアでも、サイバー攻撃の状況を一瞬で把握することができます。

また当研究所では、セキュリティ担当者にサイバーセキュリティの実戦的知識と技能を身につけていただくためのトレーニングを行っており、年間約3,000人が受講しています。

せきぐち　技術の進歩が早いですから、日々の知識・技能の更新が欠かせないのですね。それだけ、サイバー攻撃の技術の進化も速いということですね。

井上　まさにイタチごっこですね。サイバー攻撃は、無差別に攻撃してくるものが多いですが、標的をしぼって攻撃してくるケースも増えています。最近は病院への攻撃が目立ちます。保存しているデータを勝手に暗号化してロックがかけられ、「元に戻してほしかったらお金を払え！」といういわゆるランサムウェアの手口が目立ちます。

■あらゆるデバイスがサイバー攻撃の標的

井上　IoTが普及した今、ネットにつながっているすべてのデバイスが、サイバー攻撃の危険にさらされているといえます。PC・スマホはもちろん、ブロードバンドルーター・見守りカメラ・プリンター複合機などのあらゆるデバイスです。ですからセキュリティ対策は欠かせません。ただ心配しすぎる必要はなく、セキュリティアップデートをしっかりやっておけばたいていは大丈夫です。

新しい技術には、便利で生活が豊かになるという光の部分がある反面、犯罪に利用される影の部分があるということです。

せきぐち　私が使っているようなVRゴーグルもサイバー攻撃の対象になるんですか。

井上　VRゴーグルもコンピュータの一種ですから当然対象になりますね。海外の研究機関がVRゴーグルに対する攻撃事例をいくつか論文発表していますが、攻撃されるとリアル空間の部屋の様子やサイバー空間で打ち込んでいるパスワードなどの個人情報が盗み見られる可能性があります。

せきぐち　スマートフォンもそうですよね。個人情報の塊ですから。いつどこで誰とあったとか、何を食べたとかみんなわかっちゃう。ただ、こういったデジタル技術は、私のアートの根幹でもあるわけで、多くの人々に安心して楽しんでいただけるような環境を築いていきたいと思います。

井上　今怖いのは、サイバー攻撃だけでなく、SNSなどを通して拡散する偽情報や誤情報です。過去のアメリカの大統領選挙でも、意図的に偽情報が流されていたことが知られています。特にVRの世界では、没入空間で視覚情報と聴覚情報が連続的に与えられますから、変に操作されると偽・誤情報が脳にダイレクトに飛び込んできます。ですから、入出力する情報の信頼性をきちんと検証できる仕組みなどを取り入れていかなくてはなりません。

今のところVRゴーグルなどのウェアラブルデバイスがサイバー攻撃を受けた場合、脳で何がおこるかについては研究が進んでいないので、これから、この分野の研究も進めていきたいと考えています。

■脳のセキュリティ

せきぐち　生成AIの登場でフェイク映像が増えてますね。非常にリアルにできていて、ちょっと見ただけではフェイクとは気がつきません。まさに認知戦ですね。井上さんのところでは、脳の研究もしているのですか。

井上　NICTには、CiNet（脳情報通信融合研究センター、大阪府吹田市）という組織があります。サイバーセキュリティ研究所はCiNetと連携して脳のセキュリティに関する研究を始めたところです。

せきぐち　ついに脳のセキュリティまできましたか。具体的にはどういうことをやるのですか。

井上　脳で考えたことを仮想的な身体の動きとして出力し、ロボットハンドなどを動かすBCI（Brain Computer Interface）の研究が世界中で進められています。病気や高齢で体が動かなくなった人にとって大切な研究なのですが、脳の信号を直接取り出すので、究極の個人情報と言えます。NICTでは、fMRI（functional Magnetic Resonance Imaging、磁気共鳴機能画像法）を使って、人にある映像を見せたときの脳活動を解析し、そこから逆に元の映像を再構成することに成功しています。

ただ、この先、脳情報を実社会で利用していくためには、先ほどお話ししたように、脳に入出力された情報が正しいかどうか、さらには自分の脳活動に意図しないバイアスがかかっていないかなどを確認できなければなりません。脳情報システムが高度化すればするほど脳のセキュリティが重要になってくるのです。

せきぐち　それが実現するのは、だいぶ未来の話ですよね。

井上　30年後かもしれないし、10年後かもしれません。

せきぐち　えぇ〜、10年後ですか。すぐですね。今日、お話を伺って、NICTでやっている研究ってどれもとても興味深いです。脳情報通信は、これから人々がみんな関わってくることだと思います。いつか体が動かなくなる可能性は誰にもあります。そういうときに脳で「ハイ・イイエ」が示せるだけでもすごく生活が変わると思います。

サイバーセキュリティって情報を守るだけでなく、人生のすべてを守るということにつながってくるのですね。

井上　本日はどうもありがとうございました。ぜひVRアートとサイバーセキュリティとのコラボをしたいですね。

せきぐち　ぜひぜひ、こちらこそよろしくお願いいたします。

せきぐちあいみ〈左〉
株式会社MUSOU　代表取締役社長
2016年からVR空間に3Dアートを描くVRアーティストとして、様々な作品を生み出している。日本国内にとどまらず、広く海外でも活躍中。経済産業省「Web3.0時代におけるクリエイターエコノミー創出に係る研究会」、内閣府知財事務局「メタバース上のコンテンツ等をめぐる新たな法的課題への対応に関する官民連携会議」等にも幅広く携わる。

井上 大介（いのうえ だいすけ）〈右〉
サイバーセキュリティ研究所　研究所長／
サイバーセキュリティネクサス　ネクサス長
大学院博士課程後期修了後、2003年、独立行政法人通信総合研究所（現 NICT）に入所。2006年よりインシデント分析センターNICTERを核としたネットワークセキュリティの研究開発に従事。博士（工学）。

あなたがネットにアクセスするとき、サイバー攻撃は必ずあなたの傍（そば）にある

笠間 貴弘
（かさま たかひろ）
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
室長

大学院修了後、2011年にNICT入所。サイバー攻撃観測・分析、マルウェア解析、IoTセキュリティ等に関する研究に従事。博士（工学）。

「ネットは広大だわ」という名言を残したアニメ「GHOST IN THE SHELL / 攻殻機動隊」から30年がたとうとしている。アニメ公開と時を同じくしてMicrosoft Windows 95が発売され、パーソナルコンピュータを手にした人々は広大なネットの世界に足を踏み入れた。その後30年間のICT技術の進歩により、かつてSFの世界で描かれてきた技術が現実になっていく一方で、サイバー攻撃の脅威は拡大し続けている。そのような状況の中で、我々サイバーセキュリティ研究室は現在そして近い未来に発生し得るサイバー攻撃への対策技術を研究開発しています。

■14秒に1回届くサイバー攻撃通信

サイバーセキュリティ研究室では第5期中長期計画において2つの柱を軸に研究開発を行っています（図1）。「データ駆動型サイバーセキュリティ技術」においては、インターネット上で発生する多種多様なサイバー攻撃を定常的かつ大規模に観測するための技術の研究開発に注力しています。有効なサイバー攻撃対策技術を生み出すためには、サイバー攻撃の実態を把握し、マルウェア検体や攻撃通信、悪性Webコンテンツといった実データを集めて研究開発に利用することが欠かせません。例えば、我々が20年間研究開発しているダークネット観測システムNICTER（ニクター）で観測される無差別型攻撃に関連した通信は観測開始以来一貫して増加傾向を示しており、2023年には年間約6,200億パケットを観測しました（図2）。これは仮に1つのIPv4アドレスを利用してインターネットに接続している場合、平均して約14秒に1回の頻度で攻撃通信が届くことを示しています。その結果、十分なセキュリティ対策が施されていない機器をインターネットに接続してしまうと、ものの数分でサイバー攻撃の被害に遭うことになります。こうしたインターネット上の脅威の実態は実際に攻撃観測を行っている組織でないと、中々実感が湧かないのではないでしょうか。

また、サイバー攻撃はしばしば現実世界の事象とリンクする形で発生します。

図1　サイバーセキュリティ研究室の2つの柱

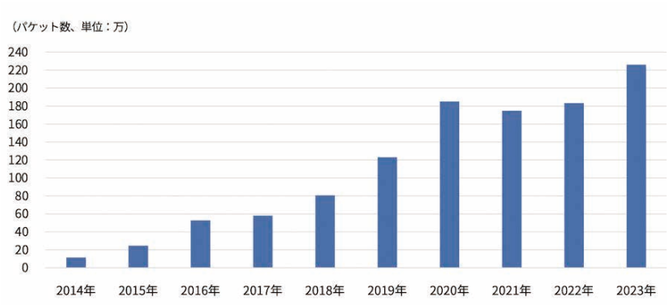


図2　NICTERで観測した無差別型攻撃関連通信の推移

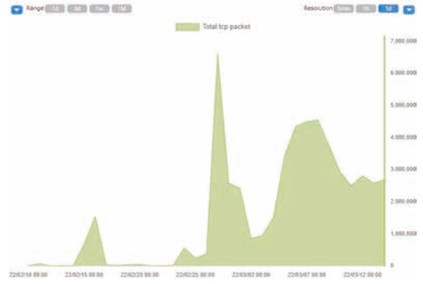


図3　ウクライナからのバックスキャッタ推移

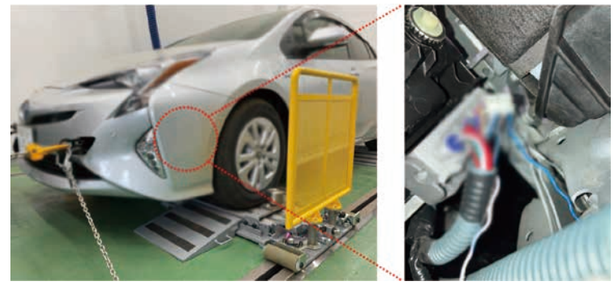


図4　コネクテッドカーの実車を用いたセキュリティ検証

2022年2月24日にロシアはウクライナへの侵攻を開始しましたが、同時期にウクライナからのバックスキャッタ（DDoS攻撃の跳ね返り）が急増していたことをNICTERは捉えていました（図3）。DDoS攻撃で狙われていた対象には政府サイトや国立銀行なども含まれており、実際にサイバー攻撃がどの程度影響を与えたかは明らかではありませんが、現実世界とサイバー空間が密接に関係している様子を示しています。

我々はこのような今まさに発生しているサイバー攻撃の実態を捉え、大規模収集したデータを基に効果的なサイバー攻撃対策技術の研究開発を推進しています。

■攻撃者の視点でリスクを探る

一方、「エマージングセキュリティ技術」においては、近い未来に発生し得るサイバー攻撃や新たな脅威に焦点を当てた研究開発を行っています。社会に新しく登場してくる技術（エマージング技術）には、往々にして既存技術とは異なる脅威が存在します。我々は攻撃者の視点からそれらの技術がいかに悪用可能か考えることで、そこに潜む脅威を特定し、リスク軽減や安全性の検証のための研究開発を実施しています。

例えば、近年ではコネクテッドカーの技術進歩が著しく、アメリカや中国をはじめとした国々では完全無人の自動運転タクシーサービスが開始されています。コネクテッドカーは従来のスタンドアローンの車とは異なり、無線通信機器や車間通信システム、各種センシングシステムなど多くの車外とのインタラクションを行うモジュールが搭載されています。サイバーセキュリティ研究室では、実際の車両を用いた検証環境を構築し、ITS（Intelligent Transport Systems）に対する攻撃の実証実験などを通じて、コネクテッドカーのリスク評価や対策手法の研究開発を行っています（図4）。

また、新たな研究テーマとして未来ICT研究所 脳情報通信融合研究センター（CiNet）と連携し、脳情報セキュリティの研究に着手しています。2021年にアメリカのSynchron社が開発した電極入り脳血管ステントを用いるBMI（Brain Machine Interface）が臨床試験を開始し、2024年にはイーロン・マスク氏らが設立したNeuralink社が麻痺患者を対象とした脳内埋込型BMIの臨床試験を開始するなど、「電脳」の世界の実現が近づいています。安価なデバイスで脳情報が容易に取得でき、脳とコンピュータが接続される世界に求められるサイバーセキュリティがどのようなものか、少なくとも現時点では我々はまだ正確な答えを持っていません。だからこそ、そのエマージング技術が広く社会に普及する前に、我々が直面するであろう脅威をいち早く特定し、セキュリティ・バイ・デザインにつなげていく取組が重要となっています。

■絶対に止めないことが重要

サイバーセキュリティ分野は、新たな技術の登場や攻撃者の進化によって状況が絶えず変化する、困難で面白い研究領域です。攻撃者は時として技術の穴だけではなく人間自身の心理的な弱点も狙ってきます。現実世界での犯罪が決してゼロにならないように、サイバー攻撃も今後無くなることはないでしょう。それでも、サイバー攻撃の被害を少しでも減らし、安心安全にICTの恩恵を享受できる社会を実現するためには、サイバーセキュリティの研究開発を絶対に止めないことが重要だと考えています。

セキュリティ基盤研究室における研究開発

篠原 直行
（しのはら なおゆき）

サイバーセキュリティ研究所
セキュリティ基盤研究室
室長

2007年から JST CREST 研究員。2009年4月より立教大学ポストドクトラルフェロー。同年7月よりNICTの研究員、2014年より主任研究員、2020年より研究マネージャー、2023年より室長。
計算数論、計算機代数、公開鍵暗号の解析の研究に従事。博士（数理学）。

量子コンピュータや機械学習等の新たな技術の登場及びその性能の向上により、様々な暗号技術及びプライバシー保護技術の必要性が高まっています。セキュリティ基盤研究室では、現代の暗号に対する量子コンピュータの脅威の評価、量子コンピュータを利用しても解読が困難な暗号の研究を進めています。また、複数の組織が持つデータを安心安全に機械学習に利活用できるDeepProtectの研究開発も進めています。

■プライバシー保護連合学習技術 DeepProtectの研究開発

機械学習は、学習データが多いほど学習の効果が高まる傾向があるため、学習データを所有する複数の組織がデータを共有することは有効であると考えられます。しかし、学習データが機微情報を含む場合は、それらを共有することは一般的に困難です。この問題を解決する一つの手段として、連合学習が挙げられます。連合学習では学習データを共有することなく各組織で機械学習を実施し、そこで得られた学習モデルを更新するために必要な情報を参加組織で共有します。しかし、その情報から学習データの情報が漏洩（ろうえい）する可能性が残ります。

この問題を解決するために、セキュリティ基盤研究室では、データを暗号化したまま加法演算が可能な準同型暗号を利用することで、学習モデルの更新に必要な上述の情報を暗号化したままモデルを更新して共有するプライバシー保護連合学習技術であるDeepProtectの研究開発を進めています。さらにDeepProtectと金融の分野の実データを用いた実証実験（図1）を進めるなど、社会実装に向けた取組も実施しています。

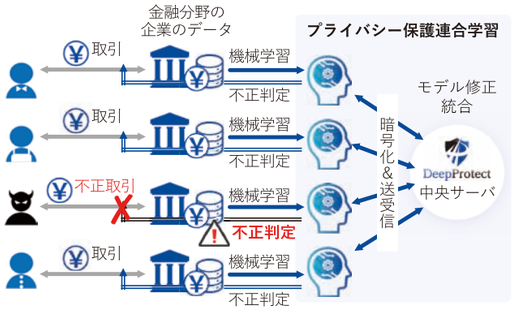


図1　DeepProtectを用いた実証実験の例

■量子コンピュータ時代に向けた暗号技術の安全性評価

セキュリティ基盤研究室では、現代の暗号技術及び将来的に利用が見込まれる様々な暗号技術の適切な実装と安全な運用に貢献するため、暗号技術の安全性及び実装性能等を評価しています。具体的には、量子コンピュータ時代にも安全に利用できる耐量子計算機暗号等の暗号技術や、現在広く使用されている RSA 暗号、楕円曲線暗号等の安全性評価に関する研究開発に取り組んでいます。またその成果を基に、電子政府推奨暗号の安全性を評価及び監視し、暗号技術の適切な実装法や運用法を調査及び検討する国のプロジェクトである CRYPTREC に貢献しています。

■量子コンピュータによる現代暗号の安全性評価

現在広く利用されている公開鍵暗号の安全性は素因数分解問題や離散対数問題と深い関係があり、これらの計算問題を解くことで暗号が解読されます。暗号解読の計算コストは問題の桁数（鍵長）が大きいほど高くなり、現在のコンピュータで数百桁の問題を解くことは現実的に不可能と考えられているため、そのような大きな鍵長を持つ計算問題が暗号に使われます。一方で、大きな計算問題でも十分な性能の量子コンピュータで高速に解けることが理論的には知られています。そのため、現在利用可能な量子コンピュータ実機により解ける鍵長の大きさを実験で確認し、現代暗号への具体的な脅威を評価する事が重要な研究課題です。

セキュリティ基盤研究室では、計算問題が量子コンピュータ実機により解けることの数学的定義を提案し、非常に小さい鍵長ですが、量子コンピュータ実機を用いて世界で初めて離散対数問題を解く実験に成功しました。本成果により、現在広く利用されている公開鍵暗号で使用される、より大きな離散対数問題を現在の量子コンピュータ実機で解くことは困難であり、現時点では現代暗号に対する量子コンピュータの脅威が生じていないことが確認されました。

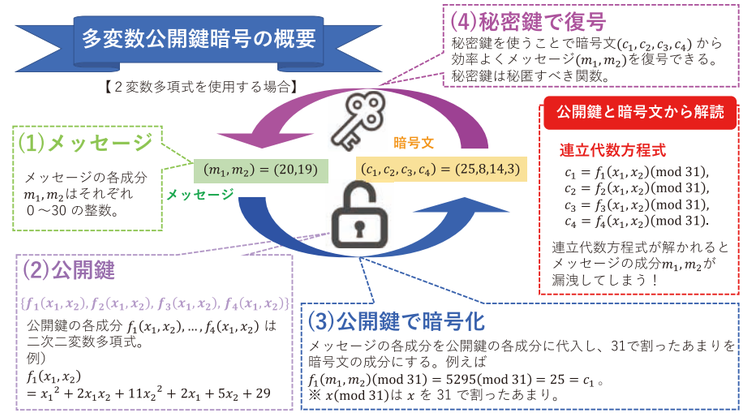


図2　多変数公開鍵暗号の概要

■耐量子計算機暗号の安全性評価

耐量子計算機暗号とは、従来の公開鍵暗号が使われている環境でも今までと同様に使用でき、量子コンピュータ及び旧来のコンピュータを用いてもその安全性を保つことができる公開鍵暗号です。具体的には、量子コンピュータ及び旧来のコンピュータを用いても高速に解く方法が発見されていない数学的な問題を安全性の根拠としている公開鍵暗号が耐量子計算機暗号とよばれています。

セキュリティ基盤研究室では、耐量子計算機暗号の主要な候補である格子暗号及び多変数公開鍵暗号を中心に安全性評価の研究を進めており、特に多変数公開鍵暗号（図 2）の解読コンテストであるFukuoka MQ Challenge において、解読の世界記録を達成しました。これらの研究で得られた知見も、後述の「CRYPTREC暗号技術ガイドライン（耐量子計算機暗号）」の策定に役立てられています。

■耐量子計算機暗号に関するCRYPTRECの活動

CRYPTREC は、電子政府推奨暗号の安全性を評価及び監視し、暗号技術の適切な実装法や運用法を調査及び検討するプロジェクトです。その事務局は、デジタル庁・総務省・経済産業省・情報通信研究機構・情報処理推進機構が務めています。CRYPTREC は暗号技術検討会の下に、暗号技術評価委員会及び暗号技術活用委員会を置いた体制になっており、耐量子計算機暗号に関する活動はNICTが主担当を務める暗号技術評価委員会及びその下に設置されている暗号技術調査WGで主に実施されています。近年の具体的な活動として、2021年度から2022年度にかけて耐量子計算機暗号の研究動向調査を実施し、その調査結果を基に「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」を策定して2023年4月に公開しています。さらに、2023年度から2024年度にかけて同様の調査を実施し、耐量子計算機暗号に関する既存のガイドラインを元に新たなガイドラインを策定する予定です。

■今後の展望

本稿ではセキュリティ基盤研究室で実施した、暗号技術及びプライバシー保護技術等の研究開発、暗号技術の安全性評価の研究に関する代表的な取組を紹介しました。DeepProtect については、金融の分野の実データを用いた実証実験を実施し、更なる改良をすべき点を発見しました。さらに、医療の分野等の新たな分野への応用の見込みとそれによって生じた新たな研究課題に取り組んでいきます。

耐量子計算機暗号については国内外で研究活動を含め種々の活動が盛んであり、特に米国の NIST（National Institute of Standards and Technology）が耐量子計算機暗号の標準化を進めており、この動向は日本で利用する耐量子計算機暗号の選定に大きな影響を与えます。NISTは2016年に耐量子計算機暗号の最初の公募を開始し、2024 年時点で幾つかの方式が標準化されつつあります。さらに、2022年に追加の公募を実施しており、これらの安全性及び実装性能の評価は2030 年ごろまで続くと考えられます。さらにそこから、実装方法の改良が進み、そのことによって改良された実装方法に対するサイドチャネル攻撃が発見されることなどを考えると、2035 年前後までは、耐量子計算機暗号の研究はセキュリティ基盤研究室で取り組むべき重要な課題と考えています。

ナショナルサイバートレーニングセンターにおける人材育成事業

園田 道夫
（そのだ みちお）
サイバーセキュリティ研究所
ナショナルサイバートレーニングセンター
研究センター長

大学院博士課程修了。2014年サイバー大学 IT 総合学部教授 を経て、2016年NICT セキュリティ人材育成研究センター長、2017 年ナショナルサイバートレーニングセンター長に就任。博士（工学）。

ナショナルサイバートレーニングセンターでは、実践的サイバー防御演習CYDER（サイダー）[*1]、実践サイバー演習RPCI（リプシ）[*2]、サイバー防御演習CIDLE（シードル）[*3]、若手人材育成事業SecHack365（セックハックサンロクゴ）[*4]という、現在4つの事業を行っています。CYDERとRPCI、CIDLEは実務者向けの実践的な演習であり、SecHack365は25才以下の若手人材（エンジニア、研究者ほか）向けの事業です。

■実践的サイバー防御演習CYDER

実践的サイバー防御演習CYDERは、当センター設立当初から行っている事業であり、毎年の動員目標が3,000人、開催回数は100回以上と、当センターの事業の中では最も規模が大きなものです。CYDERはサイバー攻撃に遭った直後の初動対応を主題とする演習であり、受講者は47都道府県各地の会場に集合して1日または2日でインシデント対応について実践的に学びます。基本的に4人1組のチームとなって各員別個の役割を担いながら、実際に起きた事件を基にしたシナリオベースでインシデント対応を進めていきます。演習環境は独自開発のCYDERANGEを用いて、仮想的な組織のネットワークを各チームに付与して調査・分析の舞台としています。

初級・入門となるAコース、中級のBコース、準上級のCコースというラインナップで、Cコースのみ2日であとは1日、加えて数時間のオンライン事前学習という構成です。

また近年の様々なニーズを受けて、2023年度より短時間でインシデント対応の基礎の基礎から学べる、オンライン独習型のプレCYDERを提供しており、サイバー攻撃に関する基礎的な知識を学んだ上で実際の事件を深掘りしたケーススタディを、複数の10分～20分程度の動画視聴形態で提供しています。さらに、集合演習と同等程度の内容をオンライン化した演習の実証実験を行っており、近い将来に提供を開始する予定です。

■実践サイバー演習RPCI

RPCIは開催形態もCYDER同様に集合演習であり、1日＋事前学習という構成で、演習環境も同様ですが、セキュリティのプロフェッショナル向けにレベルを調整したシナリオを提供しています。

■サイバー防御演習CIDLE

CIDLEは大阪・関西万博を主催する2025年日本国際博覧会協会向けに行う事業です。メインはCYDERやCIDLEと同じくインシデント対応演習になりますが、ほかにも主にメガイベント主催に関わる様々な分野・内容の座学やハンズオンを提供しています。またCIDLEでもCYDERと同様にオンライン独習型の短時間演習も提供しています。

■若手人材育成事業SecHack365

他の3つの事業とは全く異質な事業がこのSecHack365です。年6回のイベントとその間の濃密なオンラインコミュニケーションで若手を刺激し、とにかく手を動かすことができる人材を輩出しています。今年で8年目に入りますが、毎年少しずつ変化しながら進めています。

■今後の展望

CYDER、RPCIにおいては更にきめ細かくニーズを拾っていこうと思いますが、特にプレCYDERのような主催・利用者両方にとって使い勝手の良いコンテンツの充実を図ろうと思います。SecHack365は引き続きサイバーセキュリティの人材不足を解消し得るような何かを作り出す人材の、より多くの輩出を目指していきたいと思います。

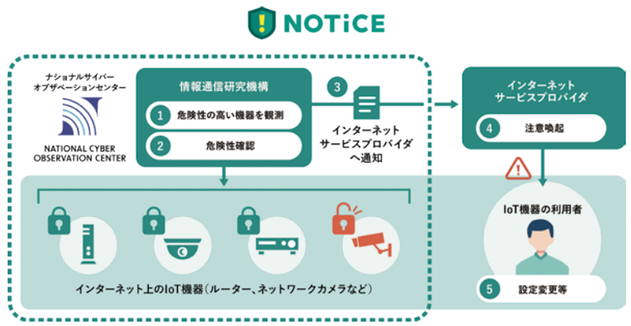
＊1　CYDER：中央省庁や地方公共団体を中心に、独立行政法人や公的組織、さらには民間企業にも展開している、実践的サイバー防御演習

＊2　RPCI：CYDERの流れをくみ、同じくインシデント対応の初動対応を主題とする演習を、国家資格である情報処理安全確保支援士向けの特定講習

＊3　CIDLE：かつて東京オリンピック・パラリンピックの組織委員会向けに演習のみならず座学やハンズオンなどを提供していたサイバー・コロッセオ事業の流れをくむサイバー防御演習

＊4　SecHack365：対象は25才以下の若手人材であり、セキュリティの課題意識を持ちながらそこにアイディアで切り込み、ものづくりで世の中を変えてくれるような人材の輩出を目的としたセキュリティ人材育成プログラム

より安心安全なIoT環境の実現に向けて



NOTICE の全体像

衛藤 将史
（えとう まさし）
サイバーセキュリティ研究所
ナショナルサイバーオブザベーションセンター
研究センター長

2005年 、NICT 入所。以降、NICTER プロジェクト、IPv6、ITS、IoT 等に関するサイバーセキュリティ技術の研究開発、国際標準化、人材育成、調査事業等の取組に加えて、イノベーション創出政策の立案等に従事。博士（工学）。

インターネットの発展に伴い、IoT 機器が私たちの生活に欠かせないものとなった一方で、IoT 機器に関わるサイバー攻撃は増加の一途をたどっており、私たちの生活に深刻な影響を及ぼしています。

このような状況をふまえナショナルサイバーオブザベーションセンター（NCO）では、総務省及び電気通信事業者（インターネットサービスプロバイダ。以下「ISP」）との連携の下、IoT 機器のセキュリティ対策向上を推進することにより、サイバー攻撃の発生や、その被害を未然に防ぐための取組NOTICE＊を推進しています。

NOTICE プロジェクトにおける NCO の主な役割は、日本国内に存在するサイバー攻撃に悪用されるおそれのある IoT 機器を発見し、当該機器の情報を ISP 等へと通知することで、これを実現するため主に以下に挙げる各種調査業務を担っています。

■ID・パスワードに脆弱（ぜいじゃく）性がある機器の調査

IoT 機器において、簡単に推測されるID・パスワード（単純な文字列や文字数が少ない等）が設定されていると、不正アクセスを受けて機器が悪用される可能性が高まります。そのため NCO では IoT 機器に容易に推測される ID 及びパスワードを入力しログインを試行する調査を行っています。ログインができた場合、その機器を脆弱性有りと判断してISP 経由で利用者に注意喚起を行い、適切なパスワードへの設定変更を促します。

■ファームウェアの脆弱性を有する機器の調査

IoT 機器のファームウェアに存在する脆弱性は、機器の機能を悪用されたり、不正な遠隔操作を許したりするなど、深刻なセキュリティリスクを引き起こす可能性があります。そのため NCO では外部から攻撃可能なセキュリティホールなどのファームウェアの脆弱性を有する機器の調査を行っています。脆弱性が発見された場合は利用者に注意喚起を行い、最新のファームウェアへの更新を促します。

■マルウェア感染機器の調査

NICTER の観測網を活用し、「Mirai」といった IoT 機器を標的とするマルウェアに感染した機器等の調査を行っています。本調査では NICTER が収集した通信データから、Mirai に感染したと疑われる IoT 機器を特定し、その感染状況や活動状況を分析します。調査の結果、感染が確認された場合は、機器の利用者に注意喚起を行い、マルウェアの駆除等の対処を促します。

■今後の展望

これらの取組により、2023 年度には ID・パスワードに脆弱性がある機器の調査においては国内に存在する設定不備の機器を 10,000 台以上発見し ISP に通知したほか、5 年以上にわたる取組の結果として、このような機器に関する注意喚起対象数は、継続的に減少傾向にあります。

一方で、現在も国内には脆弱な IoT 機器が引き続き数多く存在しており、また、新たな技術の誕生や ICT 環境の変化に伴う未知の脅威の発生に対応する必要もあることから、NCO では調査能力の向上や業務の効率化に注力しつつ、引き続きNOTICE プロジェクトを推進していきます。

＊ NOTICE: National Operation Towards IoT Clean Environment

日本のサイバーセキュリティの結節点“CYNEXアライアンス”

安田 真悟
（やすだ しんご）
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
CYNEX研究開発運用室
室長

大学院研究員を経て、2013年情報通信研究機構に入所。サイバー攻撃の再現・検証用の模擬環境構築技術に関する研究や東京2020大会関係者向けのセキュリティトレーニング事業「サイバーコロッセオ」の事業などに従事。博士（情報科学）、CISSP。

金濱 信裕
（かなはま のぶひろ）
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
CYNEX事業推進室
室長

ハードウェアベンダー、サイバーセキュリティ教材開発・講師などの仕事に携わり、2016年にNICTへ入所。これまでサイバーセキュリティ演習のシナリオ開発などに従事。趣味は世界中の「4DX」巡り。

我々サイバーセキュリティネクサス（Cybersecurity Nexus: CYNEX）は、国内におけるサイバーセキュリティに関する情報分析・人材育成等の産学官連携の中核的拠点（Nexus）として2021年に発足しました。そして、この取組を持続的に発展させるため、準備期間を経て2023年10月1日に新たな枠組みとしてCYNEXアライアンスを形成しました。CYNEXアライアンスは参画組織や構成員が課題や目的を共有して自律的に活動できる組織を目指し、後述の各Co-NexusにNICTと参画組織の有識者にチェアとして着任いただき、活動方針等を協議によって決定できるチェア制度を取り入れ、NICTと参画組織が共同で舵取りを担うことで、参画組織を巻き込んだ主体的な活動としてCo-Nexusの自走を促し、部署としてのCYNEXと事務局がそれを支援する体制としています。

■CYNEXアライアンスと4つのCo-Nexus

CYNEXアライアンスはセキュリティに関わる広範な活動を並行して進めるため、図1に示す4つのサブプロジェクト「Co-Nexus」を擁し多面的な活動を平行して実施しています。CYNEXアライアンス発足から1年、NICTと各参画組織との連携が進み、各Co-Nexusでも活動内容が増加するなど活動が活性化しています。参画組織数も急速に増加しており2024年11月1日現在、参画組織は全体で86組織になりました（表1）。

Co-Nexus A

Co-Nexus A（Accumulation & Analysis）には現在36組織が参画し、サイバーセキュリティ研究室及びCYNEXの研究開発成果を活用し、サイバーセキュリティ情報の収集・蓄積、アライアンス参画組織への解析基盤貸与・データ提供を通じて解析者コミュニティを醸成し、共同分析を進めています。

STARDUSTはサイバーセキュリティ研究室が研究開発した、主に標的型攻撃を対象としたサイバー攻撃誘引基盤です。現在20組織以上の参画組織にSTARDUSTを貸与しており、各組織が独自にサイバー攻撃の分析に利用しています。またSTARDUSTの利用組織を中心として、解析結果や知見を共有する解析者コミュニティ活動を行っています。年に4回行われる定期会合は毎回90名規模の国内の解析者が集っています。

WarpDrive Project

WarpDriveはアニメーション作品「攻殻機動隊 SAC_2045」とコラボレーションしたユーザ参加型プロジェクトです。CYNEXが研究開発を行い、アニメのキャラクター達も登場するタチコマ・セキュリティ・エージェント（タチコマSA）を無償配布することで、ユーザから提供されるウェブ媒介型攻撃に関するデータを収集・蓄積し、参画組織でデータを分析、検知技術の向上等の研究開発に活用するとともに、その成果に基づいたセキュリティアプリ機能をユーザへ提供しフィードバックを行っています（図2）。

タチコマSAはゲーム機能の搭載やセキュリティソフトとしての基本機能をブラッシュアップするなど、ユーザの長期利用を促す利用促進策を進めた結果、収集するデータ量が現在700万URL/日程度と直近2年で約7倍に増加しています。

LETTICE

LETTICEは様々な脅威情報の共同分析を目指して、Co-Nexus Aに2024年2月に新しく発足した脅威観測チームです。STARDUSTやWarpDriveでの各種観測とデータ分析では参画組織が独自に分析を行い、得られた知見を可能な範囲で共有する取組となっていましたが、LETTICEではCo-Nexus AまたはSに参画している組織から有志を募り、チームとして各種脅威を共同で分析しています。

CURE

Co-Nexus Aでは新たにサイバーセキュリティ研究室が研究開発したセキュリティ情報融合基盤“CURE”をCo-Nexus AまたはSに参画している組織向けに解放し、各組織の取得した悪性情報などを検索し、NICTが観測している各種情報基盤にどのように捕捉されているかを検索する機能を提供しています。

Co-Nexus S

Co-Nexus S（Security Operation & Sharing）では、NICT-CSIRTの片翼でもあるサイバーセキュリティ研究室の解析チームと協力し、ダークネット／ライブネットなどの定常的分析、Co-Nexus Aで蓄積した1次データや外部から入手する二次データを元に国産脅威情報の生成、情報発信をしています。また解析チームに参画企業から育成人員を受入れ、OJTやオンライン自主学習型研修により高度SOC（Security Operation Center）人材の育成を行っており、オンラインコースでは現在までに46名の修了生を輩出しています。

Co-Nexus E

Co-Nexus E（Evaluation）では、NICTの内部ネットワークをテストベッド化、参画組織が開発した国産セキュリティ製品を接続して長期運用・検証を行っています。検証ではライブトラフィックや標準的なサイバー攻撃パターンに加えて、CYNEXが有する擬似的なサイバー攻撃等を行うトップエンジニアチーム（レッドチーム）独自の模擬攻撃を併用し、製品の機能・非機能検証、既存製品との比較等を実施し、評価結果を開発組織にフィードバックすることで国産技術の研究開発支援を行います。これまで継続中を含めて8製品の検証が行われ開発ベンダに検証結果をフィードバックしています。

Co-Nexus C

Co-Nexus C（CYROP）では、NIST NICE Frameworkに準拠して、セキュリティに関わる広範な演習コンテンツを継続して開発し、それを標準的な人材育成教材として参画組織に提供する事で、国内セキュリティ人材育成の活性化を行っています。2024年度時点で提供可能な演習教材は70種類を越えており、セキュリティ知識領域の指標としているNIST NICE Frameworkに基づく領域カバー率は約50%となっています。今後は汎用的なコンテンツに加え、重要インフラなど特定の業種に特化した演習教材を作成する予定です。

■今後の展望

CYNEXは現在86参画組織と共に各Co-Nexusの活動を推進しています。これまで活動成果は参画組織内での情報共有が主でしたが、今後はCYNEXやWarpDriveのHPを活用し一般向けの情報発信にも取り組んでいく予定です。

図1　CYNEXと4つのCo-Nexus

図2　WarpDrive
（©士郎正宗・Production I.G/講談社・攻殻機動隊2045制作委員会）

図3　Co-Nexus Eの実施イメージ

表1　CYNEX参画組織数（各Co-Nexusの数字は複数のCo-Nexusに重複加盟する組織を含む）

CYNEXアライアンス全体（ユニーク総組織数）	86組織
Co-Nexus A	36組織
Co-Nexus S	18組織
Co-Nexus E	8組織
Co-Nexus C	61組織

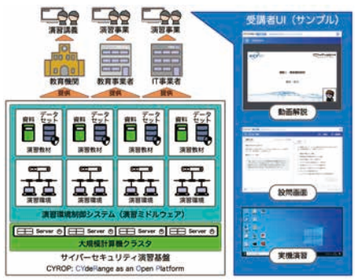


図4　サイバーセキュリティ演習基盤CYROP

サイバーセキュリティ業界で活躍する女性たちによるパネルディスカッションを実施！ NICTサイバーセキュリティシンポジウム2025開催！

サイバーセキュリティ研究所 総合企画室

毎年2月1日から3月18日は何の期間かご存じでしょうか？答えは、NISC（内閣サイバーセキュリティセンター）が定める『サイバーセキュリティ月間』です。サイバーセキュリティ研究所ではこの期間に合わせ、サイバーセキュリティの最新動向について発表や議論を行う、NICTサイバーセキュリティシンポジウムを10年以上前から毎年開催しています。余談ですが、サイバーセキュリティ月間が3月18日までなのは、“サイバー”にちなんで318となっているようです。

昨年のNICTサイバーセキュリティシンポジウム2024は、2024年２月16日に東京は日本橋にあるNICTイノベーションセンターにて、対面形式のみで開催しました。当日は全国各地の行政機関、民間企業、大学を含む研究期間等から150名近くの多くの方々にご参加いただき、会場はほぼ空席がなくなるほどの盛況となりました。

昨年は『展　～サイバーセキュリティNext Stage～』というテーマを掲げ、サイバーセキュリティ分野における研究開発の“これからの展開”について考える、3つの講演と2つのパネルディスカッションを実施しました。

中でも一番の目玉企画となったのは、サイバーセキュリティ業界で活躍する女性7名がパネルディスカッションを行うコーナー『サイバーセキュリティ女性活躍とキャリアパス』。モデレーターは佐久間萌里佳さん（株式会社incri）に務めていただき、パネリストは中島明日香さん（Elastic セキュリティリサーチエンジニア）、Yin Minn PaPaさん（横浜国立大学 先端科学高等研究院 准教授）、篠田佳奈さん（株式会社BLUE 代表取締役）、盛合志帆（NICT サイバーセキュリティ研究所長（当時））、安部小百合（NICT サイバーセキュリティネクサス 研究技術員）、松田美慧（NICT サイバーセキュリティ研究室 研究員）の6名に協力いただきました。

コーナーの冒頭では互いの名前を下の名前にちなんだニックネームで呼び合うなど、和やかな雰囲気でスタートしましたが、いざパネルディスカッションが始まると表情は一転。サイバーセキュリティ業界の課題などを、女性ならではの視点で熱く語る姿が印象的でした。質疑応答の際には、“女性の働き方”に関する質問を女性の参加者からいただくなど、ダイバーシティについて考える機会にもなり、非常に画期的な議論となりました。

さて、今年のNICTサイバーセキュリティシンポジウム2025は、2025年2月21日（金）に、昨年と同じくNICTイノベーションセンターにて開催します。今年は全国各地からより多くの方がシンポジウムに参加できるよう、対面形式に加えオンライン配信も行います。

今年のテーマは、『**継　～つづけるセキュリティ、つなぐセキュリティ～**』。内容としては、サイバーセキュリティ研究所の各部署からの最新の研究報告のほか、招待講演も予定しています。そして目玉企画としては、昨年に続き、セキュリティ業界で活躍する女性たちによるパネルディスカッション、第二弾を実施します！　昨年は盛り上がりすぎたため、80分もの時間を用意したにもかかわらず議論や質疑の時間が足りず、その議論は打ち上げ会場まで持ち越されたとか持ち越されなかったとか…ということがあったので、不完全燃焼となった議論を燃焼させるために、今年も実施します*。

ぜひ会場にお越しいただき、登壇者やご来場の方々のセキュリティに対する熱気を肌で感じていただきたいと思います。また、会場にお越しになれない方はオンラインでご参加ください。オンラインでも質問を募集いたします。皆様のご参加、お待ちしております！

（*出演者は調整中です。一部の方を除き、出演者は変更となる予定です。）

昨年実施したパネルディスカッション『サイバーセキュリティ女性活躍とキャリアパス』の様子

昨年のテーマ『展　～サイバーセキュリティ Next Stage～』

総合職の立場から考える サイバーセキュリティトレーニング事業

●経歴
2002年　東京都にて誕生
2024年　日本大学経済学部金融公共経済学科卒業
2024年　NICT入所
サイバーセキュリティ研究所
ナショナルサイバートレーニングセンター配属

杉元 沙羅
（すぎもと さら）
サイバーセキュリティ研究所
ナショナルサイバートレーニングセンター
サイバートレーニング事業推進室
一般職員

一問一答

Q NICTの職員になってよかったことは？

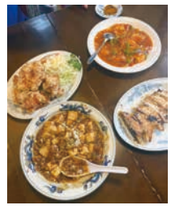
A 最先端のICT研究に携わることができ、社会に貢献できる点が大きな魅力です。普段の生活では関わることのできない研究を身近に感じることも面白いと思います。

Q NICTの総合職志望の学生さんにひとこと

A NICTでは多様な経験を通じて得られる知識やスキルが沢山あります。知りたいという気持ちを忘れずに好奇心を持ち続けてください。
NICTで皆さんにお会いできることを楽しみにしています！

Q 休日の過ごし方は？

A 大学時代の友人とご飯に行きます。最近は町中華にはまっているので、新しいお店もどんどん開拓していきたいです。



私は総合職として、ナショナルサイバートレーニングセンターの業務に取り組んでいます。センターではCYDER、RPCI、CIDLE、SecHack365の4つの事業が実施されていて、私は主にSecHack365に携わっています。SecHack365とは、“SECURITY + HACKATHON 365 DAYS”を意味する名称で、25歳以下を対象とした長期ハッカソンです。ほかにはない長期でのモノづくりの機会を得ながら、セキュリティの様々な課題にアイデアで切り込める人材「セキュリティイノベーター」の育成を目指しています。

SecHack365では、参加者の経費精算、外部事業者とのやり取り、イベントでの事務局対応を担当しています。新卒でNICTに入構したため、SecHack365やセンター内での自分自身の役割を正しく把握することが最初の仕事でした。実際の業務が始まり、SecHack365以外のセンター内業務も同時に行う必要があり、複数の仕事に優先順位をつけながら並行で仕事を進めることに慣れるまで苦労しました。SecHack365では、当初は不慣れなシステムでの経費精算に苦戦しましたが、今ではシステムや経費精算のやり方にも慣れて、ミスも減りました。SecHack365の財源は補助金なので、チーム内でのダブルチェックは必須であり、一人一人が責任をもって伝票の入力や確認をしています。そのためチーム内の連携が極めて重要だと考えています。

イベントでは参加者たちが自身の作品について生き生きと語り合う姿を目にします。テーマ設定から作品を形作る過程や1年間での彼ら自身の成長をそばで見られることが大きなやりがいです。

SecHack365のトレーニーが、自ら設定した作品テーマを追求し、形にしていくように、私も仕事に対して探求心を持ち、NICTで様々な挑戦をしていきたいです。

SecHack365では上記の5つの特徴を最大限に活用しモノづくりの機会を提供することで、「セキュリティイノベーター」としてセキュリティの様々な課題にアイデアで切り込める人材の育成を目指しています。

International Nanotechnology Exhibition & Conference

nano tech 2025

国際ナノテクノロジー 総合展・技術会議

東京ビッグサイト東ホール

ブース番号 5T-10

開催日 **2025年1月29日(水)～1月31日(金)**

https://www.nanotechexpo.jp/

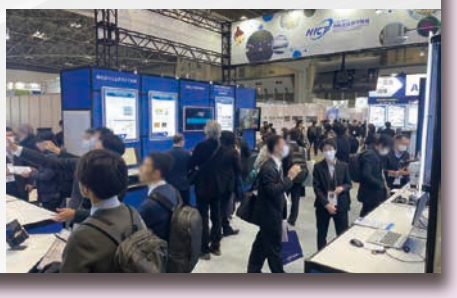
未来ICT研究所は情報通信のフロンティアサイエンス研究分野において先端的・基礎的な研究開発を行っています。
デバイス、バイオ、超高周波、量子通信、脳科学など幅広い分野での最新の研究内容を展示します。

未来ICTシンポジウム 2025

～バイオとICTの融合で拓く未来のICT～

会場 東京ビッグサイト会議棟 6F（606 会議室）

開催日 2025年1月29日(水) 13：00～17：15



MWC GSMA

今年もNICTはMWCに出展します！

3-6 MARCH 2025

Fira Gran Via, Barcelona

（スペイン バルセロナ）

BOOTH IMAGE

主な出展内容

NICTのBeyond 5G研究開発について、2030年以降の暮らしをのぞき見できるツールや、テラヘルツ波（300GHz帯）を使った4K非圧縮映像伝送システム、時空間同期された多視点大容量観測データをドローンとロボットカーが協働して無線伝送するサービスの動態展示、O-RANが国を越えて機器を制御することでシンガポールのドローンを実際に遠隔操作できるライブ体験など、盛りだくさんの内容を準備しています。

NICT NEWS 2025 No.1 通巻 509
編集発行：国立研究開発法人情報通信研究機構 広報部
発行日：令和7年（2025年）1月（隔月刊）

〒184-8795 東京都小金井市貫井北町4-2-1
TEL:042-327-5392 FAX:042-327-7587
E-mail:publicity@nict.go.jp

URL: https://www.nict.go.jp/
@NICT_Publicity
#NICT

ISSN 1349-3531 (Print)
ISSN 2187-4042 (Online)