NICT NEWS
国立研究開発法人
情報通信研究機構
No.5
2022
通巻495

FEATURE

誰も取り残さない サイバーセキュリティ

Interview

厳しさを増すサイバー攻撃 NICTのサイバーセキュリティへの取組は？

CONTENTS

NICT NEWS 2022 No.5 通巻495
国立研究開発法人情報通信研究機構

表紙写真及び左上の写真：量子セキュリティ・協創棟
訪れる人、一人一人が自分のお気に入りの場所を見つけられ、繰り返し訪れるうちに自然とその場にいる人と交流が生まれ、会話やアイデアの交換が進むような空間作りをコンセプトに建てられました。サイバーセキュリティ研究所も一部を利用しています。

柳田 敏雄（やなぎだ としお）
NICT フェロー／
未来 ICT 研究所
脳情報通信融合研究センター
R&Dアドバイザー

フェロー紹介

NICTでは、職務として行った研究開発の業務において、特に顕著な業績があると認められる者にフェローの称号を授与することとしており、令和4年5月26日、未来ICT研究所 脳情報通信融合研究センター 柳田敏雄R&Dアドバイザーに称号を授与いたしました。

柳田R&Dアドバイザーは、1998年以来、NICTにおいて、脳科学と情報科学を融合させた新しい研究分野を開拓するとともに、2011年に脳情報通信融合研究センター（CiNet）を設立し、この分野における世界的研究開発拠点形成を進めてきました。

同氏は、半導体情報処理装置などの人工システムと比べて桁違いに小さなエネルギーで動作する筋肉や細胞の生体システムが、「熱ゆらぎ」を有効活用していることを世界に先駆けて解明し、工学技術へ応用可能であることを明確に示しました。この「ゆらぎ」原理が、脳の情報処理にも適用可能であることをCiNetにおいて示しました。さらに、CiNetのセンター長として、「CiNet Brainの構築」というセンターの共通目標を設定し、多様な脳機能を統一的に理解し、応用できる研究開発をすすめています。この中から、脳情報を読み解く技術、省エネルギーで耐障害性の極めて高い情報ネットワーク制御技術、無線技術を活用したブレーン・マシン・インターフェース開発などを実現しています。

CiNetは、すでに、人間の脳を計測し解析する研究センターとしては世界的規模を有しており、わが国の有望な若手研究者を育成するだけでなく、国際交流の拠点として機能していいます。脳に学ぶ人工知能の研究にも取り組んでおり、心が通う情報通信技術の研究開発も進んでいます。このような柳田氏の独創的研究成果やリーダーシップは、恩賜賞・学士院賞受賞や文化功労者・学士院会員への選出など、多数の受賞等で国の内外から高く評価されています。

FEATURE 誰も取り残さないサイバーセキュリティ
Cybersecurity for All

Interview

厳しさを増すサイバー攻撃 NICTのサイバーセキュリティへの取組は？

コロナ禍によるリモートワークの普及、国際情勢の激変から否応なく思い知らされたサイバーセキュリテイの重要性。情報を守ることがこれほど重要だと理解された時代はないだろう。まさに今こそ情報と通信の専門研究機関であるNICTの技術が求められるときだ。サイバーセキュリティ分野でNICTが行っている取組の最前線について3人のキーパーソンに聞いた。

盛合 志帆（もりあい しほ）〈中〉
サイバーセキュリティ研究所　研究所長／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（兼務）
大学卒業後、日本電信電話（株）、ソニー（株）を経て、2012年にNICT入所、2021年から現職。暗号、情報セキュリティ、プライバシー に関する研究開発に従事。博士（工学）。

井上 大介（いのうえ だいすけ）〈左〉
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　ネクサス長／（以下兼務）
サイバーセキュリティ研究室　室長／ナショナルサイバーオブザベーションセンター　研究統括／ナショナルサイバーオブザベーションセンターサイバーオブザベーション運用室　室長
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）。

園田 道夫（そのだ みちお）〈右〉
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）。

■サイバー攻撃の現状

――最近のサイバー攻撃の傾向は？

井上　サイバー攻撃はインターネットの黎明期からありますが、20世紀が終わる頃までは愉快犯的なものが多かったです。それが21世紀に入ると金銭の詐取など特定の目的を持つものに変わってきました。攻撃側の技術はどんどん進歩していますから、守る側も進化していかないといけない。しかし、守る側の人的リソースが足りていないのが現状です。

欧米のように地続きで隣国がある地域では、軍事を含めてセキュリティ問題は重要課題として扱われてきましたが、日本は島国ということもあり、企業も国もセキュリティについて、あまり切実に感じていなかったと思います。

ところが2000年に、サイバー攻撃によって中央省庁等のウェブページが一斉に書き換えられるという事件が発生し、2011年には防衛産業が標的型攻撃を受けました。さらに2015年には日本年金機構が攻撃を受けて約125万件の個人情報が盗まれました。最近特に深刻なのは医療機関への攻撃が目立っていることです。国民の命に関わることであり、生活にダイレクトに響いてきます。

また、ここ数年はコロナ禍でリモートワークが増え、セキュリティの重要性が多くの方に認識されてきたのではないでしょうか。

――サイバー攻撃が複雑化・巧妙化していると言われますが

井上　無差別型攻撃から標的型攻撃、さらには身代金要求型へと変わってきています。また攻撃側の作業が分業化され、専用ツールも開発されているため攻撃者の裾野が広がっています。攻撃対象としては、相変わらずTCP23番ポート（Telnet、インターネット初期からある

Interview

厳しさを増すサイバー攻撃 NICTのサイバーセキュリティへの取組は？

遠隔操作プロトコル）が多いですが、全体的にIoT機器に対する攻撃が増え続けています。家庭用ルーターや監視カメラなどのIoT機器はセキュリティ設定が甘いものが多く、侵入されやすいのです。

盛合　このような攻撃に対応するためにNICTが総務省、ISP（インターネットサービスプロバイダー）とともに2019年から行っている取組がNOTICE（National Operation Towards IoT Clean Environment）です。日本国内の一億以上のIPアドレスに対して、攻撃者がIoT機器への侵入の際によく用いる約600通りのIDとパスワードの組み合わせを定め、実際にログインできるかどうか調査しています。ログインできた場合は、ISP経由でユーザーに注意喚起し、対処をお願いすることになっています。調査結果は毎月NOTICEのウェブページで公開しています。この取組によって、簡単に侵入できる脆弱なIoT機器の数はピーク時から21％ほど減りました。しかし常に新しいIoT機器がネットに接続されますから、このような取組を続けることは重要です。

井上　NOTICEが始まったのは2016年に家庭用ルーターやネットワークカメラなどのIoT機器を狙うMiraiというマルウェアが登場し、大きな被害をもたらしたことがひとつのきっかけです。このマルウェアは弱いパスワードを狙って侵入してきて、DDoS攻撃（Distributed Denial of Service attack、大量のデータを送りつけてシステムをダウンさせる攻撃）を行ったり、他の機器への侵入のための踏み台にもなります。

■安全なデータ利活用や将来に向けた暗号技術の重要性

――暗号技術の研究も進められていますね

盛合　個人情報や機密情報は確実に守られなければなりませんが、一方でプライバシーや機密性を守りながら活用すれば、社会を便利にできます。例えば異なる企業が持つデータを利活用することで、いろいろな社会問題の解決につなげられます。

そこで私たちはDeepProtectというプライバシー保護連合学習技術を開発しました。連合学習（Federated learning）とは、データを分散させたまま機械学習を行うAI技術で、組織の枠を超えて機密性の高い情報を活用してプライバシーを保護したまま安全に機械学習が行えます。

具体的な例でいいますと、複数の銀行の預金者の入出金データを学習しておくことで、疑わしい取引があった場合に素早く検知できます。より多くの銀行のデータを集めれば、検知精度を上げることができるのです。

これまで、複数の銀行とともに実証実験を行い、高精度のモデルが作れるようになっており近い将来実運用を目指しています。

もう一つ大きな柱は、まもなくやってくる量子コンピュータ時代に対応した暗号技術に関する研究です。現在使われているRSA暗号は大規模量子コンピュータが実現すると破られることがわかっているので、量子コンピュータでも解けない新しい暗号技術（PQC, Post-Quantum Cryptography）が求められているのです。現在、米国標準技術研究所NIST（National Institute of Standards and Technology）がPQCの標準化作業を行っていまして、標準暗号を発表する直前段階になっています。

■サイバーセキュリティの結節点を目指すCYNEX（サイネックス）

――NICTのサイバーセキュリティへの取組としてサイバーセキュリティネクサス「CYNEX」がありますが、これはどういうものでしょうか

井上　CYNEXは低迷するセキュリティ自給率の向上に向け、サイバーセキュリティ分野の結節点となることを目指して作った組織で、今中長期計画がスタートした2021年4月から動き始めています。これまで、NICT内ではサイバーセキュリティ研究室がサイバー攻撃のデータを大量に収集・解析し、ナショナルサイバートレーニングセンターではセキュリティ関係の人材育成を担当していましたが、新組織はこれらを基に産学官の結節点を形成し我が国のサイバーセキュリティ対応能力を向上させていきたいと考えています。

CYNEXでは、4つのプロジェクトを同時に推進しています。①データ収集と解析。②セキュリティ・オペレーションを担うSOC（Security Operation Center、組織内のセキュリティ運用組織）人材の育成と情報発信。③日本製セキュリティ製品の能力検証。④サイバーセキュリティ演習基盤のオープン化による人材育成支援です。

初年度で既に30以上の組織に参画いただき、CYNEXが産学官の結節点として機能し始めており、データ収集・解析から人材育成までスピードアップして行えるようになります。

NICTにおけるサイバーセキュリティ分野の取組

■サイバーセキュリティ人材育成

――日本のサイバーセキュリティ人材は不足していると言われますが対応は

園田　私が担当しているナショナルサイバートレーニングセンターでは3つの事業を行っています。1つは実践的サイバー防御演習CYDER（サイダー）です。官公庁及び民間のセキュリティ担当者を受講生として、サイバー攻撃をシミュレーションし、対応を実際に学習してもらいます。年に3,000人くらいの人が受講しています。

2つめが、実践サイバー演習RPCI（リプシィ）です。これは、情報処理安全確保支援士という国の資格の更新用の演習です。CYDERよりも、技術的難易度が高くなります。３つめがSecHack365（セックハックサンロクゴ）で、大学院生・大学生・高専生など若い人向けの講習で、セキュリティイノベーターの育成を目指しています。

園田　国内で10万人を超えるセキュリティ技術者が不足しているといわれます。そもそも日本の情報通信分野全体で見ても、大学等の卒業生の数は年間数万人程度ですので、これまでのやり方だけでセキュリティ人材不足を解消することは容易ではありません。若手人材の育成を行いつつ、新しい技術開発によってセキュリティの業務のハードルを下げて、他分野の人材がセキュリティ分野に参入しやすくすることも必要です。

井上　そのためには、セキュリティの自動化技術の研究開発が重要となります。自動化の鍵を握るのは、日々の観測・分析活動で異変の兆候や侵入を素早く検知する技術です。一日何億件にもなるセキュリティアラートを人手で解析するのは不可能です。そこでAIとサイバーセキュリティの融合研究も進めています。

■ダイバーシティ＆インクルージョンという考え方

盛合　セキュリティ人材の裾野を広げ、さらに新しい技術の開発を行っていくためには、女性研究者や外国人研究者など幅広い人材に向けて門戸を開く必要があります。

サイバーセキュリティ研究課題の観点からいいますと、ユーザブルセキュリティという分野が注目されています。人間の行動様式・思考様式からセキュリティを考えようという分野です。例えばSNSの不確かな情報に接した場合にどう対処すればいいかといったことなどですが、この分野では心理学や社会学を学んだ方にも加わってもらっています。

ダイバーシティ＆インクルージョン（国籍・性別・年齢などの違いを超えた包摂性）のある環境を構築し、様々な研究者の力をあわせて研究開発を進めることが大切だと考えています。

――NICTがサイバーセキュリティ分野で目指す方向は

井上　セキュリティは、よくいたちごっこだと言われます。対策を考えても次から次へ新しい攻撃手法が出てきます。これに根気強くつきあっていくことが大切だと思います。そのような長期的な視点で研究開発に取り組めることは、我々が国立の研究機関であるからこその強みです。

園田　人材育成という面から見ると、人材の供給とセキュリティ人材の裾野を広げることが重要なのですが、一方で特に秀でた力を持ってるスーパーハッカーのような人材を発掘していくことも大切だと思います。

盛合　サイバーセキュリティ技術で、社会の安心安全を守っていくことが大切です。多様な人材を巻き込んでダイバーシティ＆インクルージョンで貢献していきたいと思います。

データ負けのスパイラルから脱却するための実践的サイバーセキュリティ研究

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　副室長
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セキュリティに関する研究に従事。博士（工学）。

高橋 健志（たかはし たけし）
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　副室長
タンペレ工科大学、株式会社ローランド・ベルガーを経て、2009年よりNICTに勤務。サイバーセキュリティ及びAI技術に関する研究開発に注力。博士（国際情報通信学）。

井上 大介（いのうえ だいすけ）
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）。

次のニュースです。XX社が標的型サイバー攻撃を受け70万件の顧客情報が漏洩したことが明らかになりました。関係者の話によると…。

今やサイバー攻撃に関する話題は巷にあふれ、私たちは日々新たなサイバー攻撃の脅威にさらされています。巧妙化・多様化が進むサイバー攻撃に対抗するため、我々は国の研究機関という中立性を生かし、データ駆動型サイバーセキュリティ技術とエマージングセキュリティ技術の2つの柱を基に実践的サイバーセキュリティ研究を加速させています。

■サイバーセキュリティはデータが命

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）。

サイバーセキュリティはデータが命であり、いかに鮮度の高い実データを大規模かつ定常的に収集・蓄積する仕組みを構築できるかが研究開発の重要なポイントになります。残念ながら、サイバーセキュリティ分野では海外製のセキュリティ製品が市場を占めていて、国内にサイバーセキュリティの実データが集まりにくい状況になっています。データが集まらないことで研究開発や人材育成が効果的に進まず、その結果として国産技術が生み出せずデータは増々集まらないという負のスパイラルに陥っています。

そこで我々は、このスパイラルから脱却するため、20年近く継続しているダークネット観測データ（図2）をはじめとし、ハニーポットで収集したマルウェア検体、セキュリティアプライアンスのアラート情報、悪性サイトのURL情報や脅威情報など、多種多様なデータを大規模かつリアルタイムに収集するための観測技術の研究開発を進め、セキュリティ情報融合基盤CURE（Cybersecurity Universal Repository）の構築を進めています（図3）。CUREに蓄積されたセキュリティビッグデータを基に、可視化技術やAI技術を駆使した自動対策技術の確立を目指すデータ駆動型サイバーセキュリティ技術の研究開発に取り組んでいます。

その一方で、新たに社会に登場する技術には新たなセキュリティの脅威が付きものです。我々は最新の通信機器やコネクテッドカー、5G/Beyond 5Gなどのエマージング技術に対応したセキュリティ検証技術の研究開発にも取り組んでいます。一例として、電子回路やチップ、実車等のハードウェアに対するセキュリティ検証環境やエミュレーション技術を活用した5Gの検証ネットワークを構築し、脅威分析や攻撃シナリオの評価を行うことでセキュリティ課題の抽出と対策につなげています。また、セキュリティでは人間（ユーザ）も重要な要素になります。ユーザの行動様式やメンタルモデル、意思決定プロセスを分析し、ユーザビリティを損ねることなくセキュリティを実践するためのユーザブルセキュリティの研究開発も進めています。

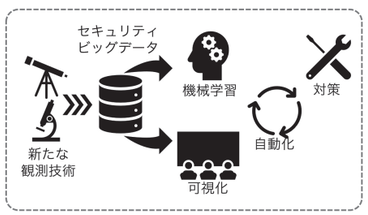


図1　サイバーセキュリティ研究室の2つの柱

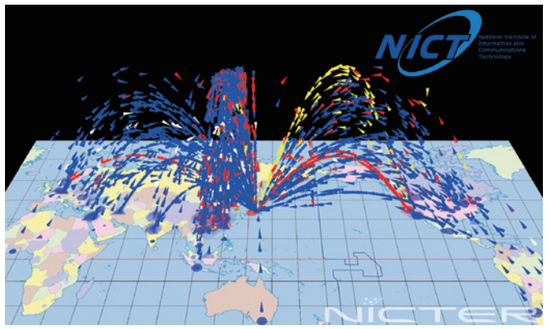


図2　サイバー攻撃観測・分析システムNICTER

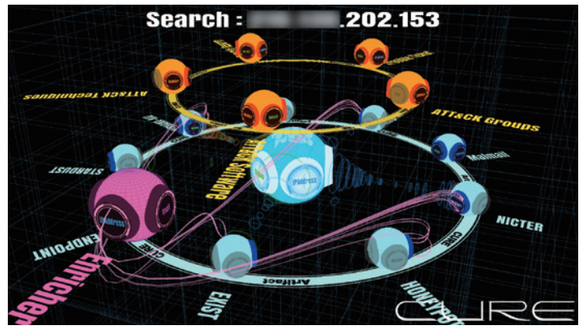
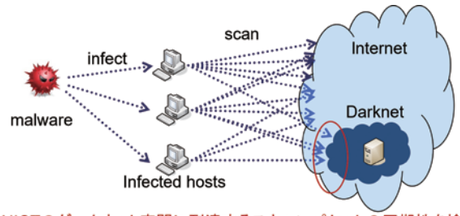


図3　サイバーセキュリティ情報融合基盤CURE

■AI技術によるセキュリティオペレーション自動化

サイバー攻撃から組織を守るためには、適切なセキュリティオペレーションによってセキュリティインシデントを一早く検出し、状況を把握することが重要になります。しかし、クラウドの利活用やテレワークが進んだ結果、従来の自社ネットワークとインターネットの境界で攻撃を防ぐ境界防御モデルは限界を迎えていて、セキュリティオペレーションでは多種多様なデータを統合的に分析しなければならず、負担が増大しています。我々は、収集したセキュリティビッグデータに対して機械学習をはじめとする各種AI技術を適用し、セキュリティオペレータやアナリストの持つ高度なノウハウをシステム化することで、セキュリティオペレーションの自動化とDXの実現を目指しています。

中でも総務省の委託研究プロジェクトMITIGATEでは、国内の大学及び企業と連携し、ダークネット分析やマルウェア収集・解析、脅威インテリジェンス分析、ダークネット分析など人手を介さずに連動して実施することで、質の高いセキュリティレポートを自動生成しオペレータの負荷を大幅に軽減する、ハイブリッド分析プラットフォーム技術を開発しています。本技術により、一例ですが、新たなマルウェアの発生をいち早く自動的に検知し、そのマルウェアを特定の上、そのマルウェアの挙動解析結果、コード分析結果、攻撃対象となっている脆弱性の情報、そして当該マルウェアの詳細レポートをリアルタイムに収集・統合して掲示することが可能になります。また、この新たなマルウェア発生の検知は、独自の技術により実現しており、マルウェアに感染した端末から発せられるスキャンの同期性を検出することにより実現しています（図4）。ほかにも多数のセキュリティアラートから対処を要する重要なものを抽出する技術や、IoTマルウェアを高速かつ高精度にクラスタリングすることで、詳細分析が必要な新たなマルウェアを迅速に発見する技術など、より多くのオペレーションを支援できる技術の研究開発を進めています。また、システムが下した判定結果の妥当性を説明・検証可能であり、わかりやすく掲示できる技術の実現も重要な課題です。



NICTのダークネット空間に到達するスキャンパケットの同期性を検知
図4　新たなマルウェアの発生を早期に自動検出する技術

■国内外の研究連携によって世界的な研究開発拠点を目指す

サイバー空間は広大で、データ収集や人材の確保含めて我々が単独で実施できる研究開発には限界があります。そこでサイバーセキュリティ研究室では、国内外の組織との研究連携を積極的に進めています。例えば、NICTERのダークネット観測では30万IPv4アドレスの世界最大級の攻撃観測網を構築していますが、この観測網は世界10か国以上に渡る数十組織との連携によって実現しています。複数地点の観測結果を集約することで、サイバー空間の状態をより精緻に分析・把握できるようになりました。こうして集めたデータは組織間で利活用することが重要ですが、一方で他組織にそのまま開示できない機微な情報も存在します。そのため、台湾の連携組織との間では、お互いのデータの学習結果のみを共有することにより、インターネット上でのマルウェア活動の発生検知を実現する方式を研究開発するなど、安全かつ効果的なセキュリティ関連情報の利活用も進めています。さらに、データだけではなく人材育成の観点でもインターンや研修生の受入を積極的に実施しており、世界的な研究開発拠点となることを目指しています。

■今後の展望

本中長期計画では、サイバーセキュリティ研究室はデータ駆動型サイバーセキュリティ技術とエマージングセキュリティ技術の両輪の研究開発を実施していきますが、その大前提となるのは、我々が従来から地道に実施してきたデータ収集・蓄積と分析技術の継続的発展です。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。その中で我々は常に状況を見定めて目標を進化させ、攻めの研究開発を通じて国産のセキュリティ技術を輩出していくのと同時に、国際連携も積極的に牽引しグローバルレジリエンスを構築していこうと考えています。

安全なデータ利活用技術と量子コンピュータ時代に向けた暗号技術の安全性評価

江村 恵太（えむら けいた）〈左〉
サイバーセキュリティ研究所
セキュリティ基盤研究室
研究マネージャー

大学院博士課程修了後、JAISTポストドクターを経て2012年NICT入所。暗号理論・暗号応用に関する研究に従事。博士（情報科学）。

篠原 直行（しのはら なおゆき）〈右〉
サイバーセキュリティ研究所
セキュリティ基盤研究室
研究マネージャー

大学院博士課程修了後、JST CREST研究員等を経て2009年NICT入所。暗号の安全性評価に関する研究に従事。博士（数理学）。

野島 良（のじま りょう）
ネットワークセキュリティ研究所
セキュリティ基盤研究室 室長

2006年、NICTに入所。情報セキュリティ技術、特にプライバシー保護技術の研究開発に従事。博士（工学）。

セキュリティ基盤研究室では、耐量子計算機暗号等を含む新たな暗号・認証技術やプライバシー保護技術の研究開発を実施し、その安全性評価を行うとともに、安全な情報利活用を推進しています。

■安全なデータ利活用技術

暗号化ストレージの利便性を向上させる技術

クラウドストレージのようなシステムのプロバイダにとって、エンドユーザのみが暗号化／復号できるエンドツーエンド暗号化（E2EE）でセキュリティを高めると、サーバ側ではデータが見えず、利用者に検索機能などのサービスを提供できないというジレンマがあります。当研究室では、検索可能暗号を用いたセキュアストレージ・チャットシステムの研究を行っています。サーバに保存されたファイルやチャットメッセージは暗号化され、同時に暗号化ファイルに対する検索が可能です。さらに検索するキーワードもサーバには漏洩（ろうえい）せず、ファイル・メッセージに関する情報が漏洩するリスクを減らすことができます。

アクセス制御・改ざん防止技術

当研究室では、宇宙機の乗っ取り防止による飛行の安全確保、宇宙機から伝送される飛行状況や学術的・商業的価値の高いデータの保護を目的とした暗号技術の研究開発を行っています。併せて実際の宇宙ロケットを使用しての実証実験を進めており、2021年には機体から地上局への飛行状況の伝送において情報理論的に安全な実用無線通信に成功しました（報道発表2021年8月17日：観測ロケットMOMOv1で情報理論的に安全な実用無線通信に成功（https://www.nict.go.jp/press/2021/08/17-1.html））。またある秘密情報を知っていることのみを証明するゼロ知識証明について、当研究室では、この技術の適用範囲の拡張及び既存方式に比べ、よりコンパクトな証明サイズを可能とする構成方法について研究を進めています。またその応用として、自身がある権限を持つこと（例えばアクセスを許可されたメンバーであること）を自身を特定することなく証明する匿名認証技術の研究開発を行っています。特に追跡可能性／失効可能性と匿名性とを両立する技術や、その応用としてブロックチェーンにおけるプライバシー保護について研究開発を行っています。

複数組織にまたがるデータやヘルスケアデータの安全な利活用技術

当研究室では、準同型暗号を応用し、それぞれの組織が持つ個人情報などの秘密データを外部に開示することなく、ビッグデータを暗号化したまま安全に解析・検知できるプライバシー保護連合学習システムDeepProtectの研究開発を行っています。この技術の活用先として、複数銀行間にまたがるデータの解析により、マネー・ロンダリング、不正送金、振り込め詐欺などの金融犯罪対策が考えられます。また、ヘルスケアの分野において、研究室ではプライバシー保護の観点で、データ分析前に行う匿名加工における安全性を保証する技術について研究を行っています。さらに、個人データ収集時のセキュリティ・プライバシー対策を個人にとって真にわかりやすく、効果的に受け止められるものにするために、プライバシーポリシーの解析や特徴比較を行い、ユーザブルセキュリティの向上に貢献する研究に取り組んでいます。

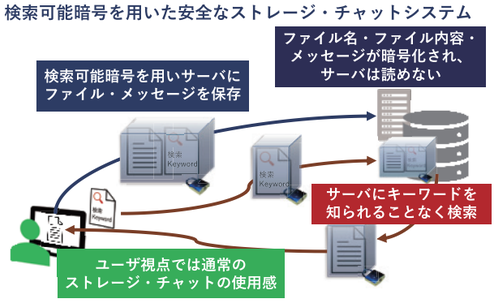


図1　検索可能暗号を用いた安全なストレージ・チャットシステム

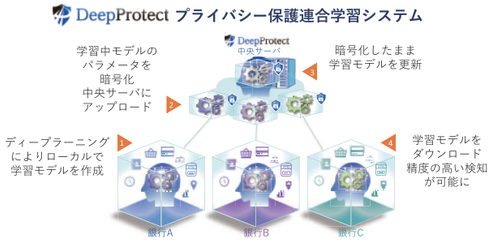


図2　プライバシー保護連合学習システム DeepProtect

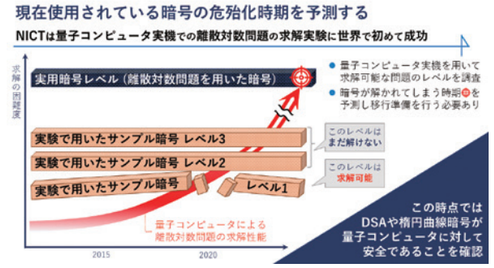


図3　離散対数問題に基づく暗号の危殆化時期を評価

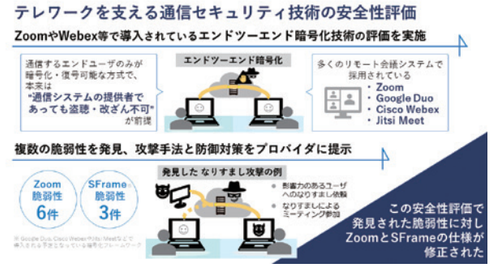


図4　テレワークを支える通信セキュリティ技術の安全性評価

■量子コンピュータ時代に向けた暗号技術の安全性評価

現代暗号に対する量子コンピュータの脅威の評価

近年、世界中の組織で量子コンピュータの開発が活発に行われ、社会還元に向けた応用研究が進められています。その反面、十分な性能を持つ量子コンピュータが整数の素因数分解や離散対数問題を解く計算を効率よく実施できるという理論的な結果から、現在広く利用されている暗号方式（RSA暗号、楕円曲線暗号、DH、DSA等）の安全性が危殆（きたい）化することが懸念されています。ただし、現在利用されているRSA暗号では2048 bit以上の合成数を使用しているのに対し、現在の量子コンピュータを用いた数値実験で素因数分解できた最大の合成数は21であるため、現時点では直接の脅威とはなっていません。当研究室では慶應大学、三菱UFJフィナンシャル・グループ、みずほフィナンシャルグループらとの共同研究で、量子コンピュータを用いて世界で初めて2 bitの離散対数問題を解くことに成功し、現時点ではDH及びDSAや楕円曲線暗号に対する量子コンピュータの脅威が無いことを確認しました。また、この成果はDH、DSA、楕円曲線暗号が危殆化する時期の算出に貢献しています。

耐量子計算機暗号（多変数公開鍵暗号）の安全性評価

量子コンピュータ及び現在のコンピュータを利用しても解読が困難な暗号は耐量子計算機暗号とよばれ、その研究開発と標準化が世界的に進められています。耐量子計算機暗号の代表的な候補として多変数公開鍵暗号が挙げられます。多変数公開鍵暗号の安全性は連立代数方程式を解く計算の困難性に依存しており、主に変数の個数が大きいほどその困難性は高まります。多変数公開鍵暗号の安全な運用には、現在最高の技術力で解ける連立代数方程式の変数の個数を評価する必要があります。当研究室では東京都立大学との共同研究で、多変数公開鍵暗号の国際的な解読コンテストにおいて37変数の連立代数方程式を解く世界記録を達成し、多変数公開鍵暗号の安全な暗号パラメータの算出に貢献しています。

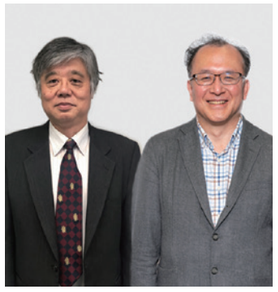
E2EEの安全性評価

コロナ禍を経て、リモート会議システムは急速に普及しました。一方で、当初これらのセキュリティに不安を持つ声もありました。NICTではこれらのシステムの安全性評価を行い、安心安全な運用の実現に貢献しています。当研究室では兵庫県立大学、NECと共同で、Zoomに導入されているエンドツーエンド暗号化技術やGoogle Duo、Cisco Webex、Jitsi Meetなどで導入予定のエンドツーエンド暗号化技術SFrameに対して安全性評価を実施しました。ZoomとSFrameの安全性評価ではそれぞれ複数の脆弱性を発見し、これらの脆弱性を利用した攻撃手法とその防御対策について、ZoomとSFrameの設計者に脆弱性報告を実施しました。脆弱性報告を実施した後、ZoomとSFrameの仕様が速やかに修正されていることを確認しました。

誰一人取り残さないサイバーセキュリティの実現に向けて

NICT ナショナルサイバートレーニングセンターの取組

花田 智洋（はなだ ともひろ）
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研究室 室長
2017年NICT入所。前職はITベンダーに勤務し、銀行基幹系システムの開発・運用にプロジェクトマネージャーとして携わる。現在は研究室長としてCYDER、SecHack365、CYDERANGE開発等の事業に携わる。SECCON実行委員長。



島田 弘一（しまだ こういち）〈左〉
同研究所　同センター
サイバートレーニング事業推進室 室長
1980年郵政省電波研究所（現NICT）入所。"事務面、ロジ面等、事業に関わるよろずの対応をきめ細やかに遂行するセンターの事業を支える組織"の長として屋台骨を支えている。

園田 道夫（そのだ みちお）〈右〉
同研究所　同センター 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（通称：ナショトレ）はサイバーセキュリティの人材育成をミッションとする組織です。情報通信分野を専門とする我が国唯一の公的研究機関であるNICTの技術的知見、研究成果、研究施設等を最大限に活用し、実践的なサイバートレーニングを企画・推進する組織として2017年4月1日に設置されました。

現在のナショトレは、実践的サイバー防御演習「CYDER」（サイダー）、実践サイバー演習「RPCI」（リプシィ）、「SecHack365」（セックハックサンロクゴ）の３つの事業運営を行っています（図1）。以降の節では、各事業の特長とNICTの強みを記します。

■実践的サイバー防御演習「CYDER」（サイダー）

CYDERは国の機関、地方公共団体及び重要インフラ事業者等の情報システム担当者等が、組織のネットワーク環境を模擬した環境で、実践的な防御演習を行うことができるプログラムを提供することにより、数千人規模でセキュリティオペレーターを育成する事業です。

NICTの強みである大規模計算機環境を活用して実際の組織を模した環境を構築し、サイバー攻撃に関する長年の観測・研究を活かしたシナリオによる最大4名のグループワークによって、リアリティのあるインシデントハンドリングが体験できます（図2）。受講直後に発生したインシデント対応に役立った例もあり、より応用が利くものとするための繰り返し受講を推進すべくコンテンツの改良を積み重ねています。

CYDERは2013年度に総務省の実証実験として開始され、その後事業主体をNICTへ移管し、実施体制の強化や実施内容の充実を行ってきました。現在では、全国47都道府県、年間100回、3,000人程度が受講可能な規模で運営しています。これまでの演習方法は集合演習のみでしたが、ナショトレが開発した演習プラットフォームCYDERANGE（サイダーレンジ）の研究・開発成果を活用し、オンライン演習も提供できるようになりました。

■実践サイバー演習「RPCI」（リプシィ）

公的機関初の情報処理安全確保支援士（登録セキスペ）向け特定講習[*1]として、2021年度から実践サイバー演習「RPCI」の提供を開始しました。RPCIはこれまでCYDERで培ってきたNICTの強みである大規模環境と実機演習のノウハウを活かし、登録セキスペ特定講習向けのカリキュラムとシナリオを構築した、技術に寄った講習を希望する受講者のニーズに対応する講習です。

RPCIの受講者は、CYDER同様に仮想組織のネットワークをシミュレートしたリアリティのある演習環境上で擬似的に発生させたサイバー攻撃に、最大4人一組のCSIRT[*2]としてチームで対処します。実際に起こり得る攻撃シナリオで、実機を用いてインシデントハンドリングのプロシージャ（手順）を1から10まで学ぶことができます。

National Cyber Training Center

図1　ナショナルサイバートレーニングセンター3つの事業

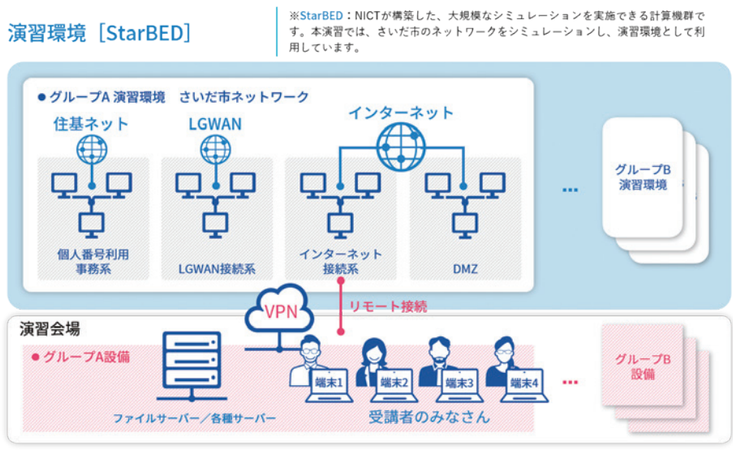


図2　各グループそれぞれに提供するネットワーク構成例

図3　2022年度SecHack365年間プログラム

ことができます。

演習提供から間もないRPCIですが、受講者からは「普段の業務では行うことのできない実習（ハンズオン）が非常に貴重な経験となった」「同じチームの方々や講師の方と会話することで、学びながら実践的な経験を積めた」等、普段の業務ではなかなか体験が難しい実践に近い形での演習を提供できています。また、夏に開催した演習受講者からは「講師チューターのサポートが良く充実した演習だった」旨の暑中見舞いが届きました。

RPCI受講を通じて登録セキスペの方がインシデントハンドリング能力を向上することで、安全安心な社会の実現に貢献することを目指しています。

■「SecHack365」（セックハックサンロクゴ）

自ら手を動かし、セキュリティに関わる新たなモノづくりができる人材（セキュリティイノベーター）の育成に向けて、若年層のICT人材を対象に、NICTの持つ長年の研究開発のノウハウや、実際のサイバー攻撃関連データとそれらを安全に利用して研究開発が行える環境を活かした、1年をかけて本格的にセキュリティ関連技術の指導を行うプログラムがSecHack365です。

ICT分野・セキュリティ分野等の第一線で活躍するトレーナー陣や同プログラムを修了したアシスタントが、25才以下の若手ICT人材を対象に選抜した約40名に対し、セキュリティに関する技術などの研究開発や、一般的なモノづくりにおけるセキュリティ面の磨き上げを通年で支援します（図3）。

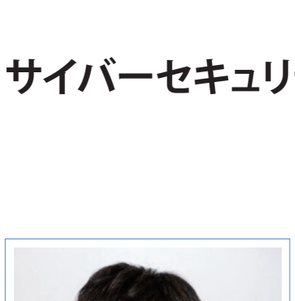
モノづくりのアプローチが異なる複数のコースを設置し、応募時に自らが望むコースを選択することでミスマッチを抑制しています。ゲスト講演や習慣化活動等の全体指導でのインプットやコースごとの特長のあるコースワーク活動を提供します。SecHack365の受講者（トレーニー）は、他のトレーニーと作品作りや発表等の議論により、自らが設定したテーマを磨き上げて、作品の完成を目指します。

＊1　特定講習：セキュリティに係る最新の知識・技能を備えた専門人材の国家資格「情報処理安全確保支援士（登録セキスペ）」の更新にあたり、3年に1回受講が必要となる講習で、経済産業大臣が定めるもの。

＊2　CSIRT:「Computer Security Incident Response Team」の略。情報セキュリティに関わるインシデントに対処する組織のこと。自組織のインシデント（事件や事故のこと）に対処する以外にも、インシデント情報、脆弱性情報、攻撃予兆情報の収集・分析、対応方針や手順の策定などを行う。

サイバーセキュリティの結節点を目指して

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研究室 兼 サイバーセキュリティネクサス 研究マネージャー
2013年NICT入所。ネットワークシステムの大規模検証、サイバー攻撃の検証、セキュリティトレーニング演習用各種模擬環境の構築・駆動技術の研究開発に従事するとともに、Hardening Project、Cyber colosseo、SecHack365などNICT内外のセキュリティ人材育成プロジェクトに従事。



井上 大介（いのうえ だいすけ）
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　ネクサス長／
サイバーセキュリティ研究室　室長
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）。

日本のサイバーセキュリティの現場では海外のセキュリティ技術を導入・運用する形態が主流となっており、セキュリティ自給率は危機的な水準です。セキュリティ技術を過度に海外依存する状況は日本の国際競争力の低下を招いており、2019年の内閣サイバーセキュリティセンター（NISC）のサイバーセキュリティ研究開発戦略専門調査会[*1]でも、国産技術・産業の育成の重要性が指摘されています。

■「データ負けのスパイラル」解決のための４つのCo-Nexus

サイバーセキュリティ分野では、サイバー攻撃に関連した「データを大量に集める」こと、データを分析し対処する「人」と「技術」を育成することが必要です。AI／機械学習などの技術の発展に伴い、サイバーセキュリティの世界でもビッグデータを活用した分析技術の研究開発が盛んに行われています。しかし、セキュリティに関する実データは機微情報であるため共有が難しく、セキュリティ市場で大きなシェアを持つ海外セキュリティベンダが実データを大量に収集・保有し、それがビジネス優位性にもなっています。その結果、海外セキュリティ製品に依存している国内ベンダは、自社で実データを集める方法に乏しく、国産技術の研究開発をしたくても利用可能な実データがないため、研究開発が停滞する「データ負けのスパイラル」の悪循環に陥っています。

この課題を解決するために、2021年4月にサイバーセキュリティネクサス（Cybersecurity Nexus: CYNEX）がサイバーセキュリティ研究所の中に新設されました。負のスパイラルを１つの問題解決で逆転するのは難しく、多面的に取り組む必要があります。CYNEXではサイバーセキュリティ研究室で培った研究開発成果、セキュリティ情報収集基盤と、ナショナルサイバートレーニングセンターで培ったセキュリティ人材育成のノウハウを結集し、国内民間企業や教育機関、政府機関などの結節点（Nexus）となるアライアンスを形成します。そして、4つのサブプロジェクト「Co-Nexus」を立ち上げ（図1）多面的な活動を並行して実施し、我が国のサイバーセキュリティ対応能力の向上とスパイラルの逆転を目指します。

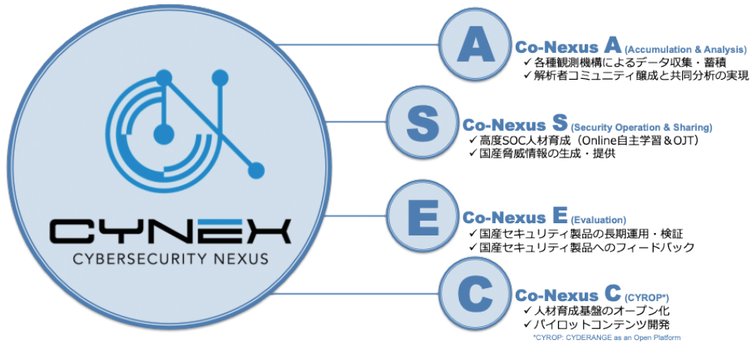


図１　４つのCo-Nexus

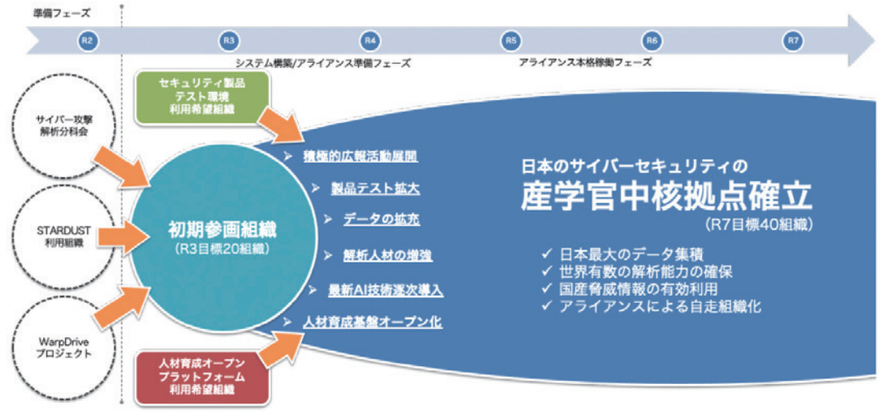


図2　CYNEXの計画タイムライン

■Co-Nexus A

Co-Nexus A（Accumulation & Analysis）では、サイバーセキュリティ研究室の研究開発成果であるサイバー攻撃誘引基盤「STARDUST」や、攻殻機動隊 SAC_2045とタイアップしたWeb媒介型攻撃対策プロジェクト「WarpDrive」などを活用し、サイバーセキュリティ情報の収集・蓄積・分析やCYNEX参画組織への分析基盤の貸与を行うことで、国内の解析者コミュニティの醸成と共同分析の実現を目指します。

■Co-Nexus S

Co-Nexus S（Security Operation & Sharing）では、セキュリティオペレーションセンター（SOC）向けの高い技術力を持つ人材を育成するため、オンライン自主学習型の教育プログラムを参画組織向けに提供し、さらにCYNEX解析チームでのオン・ザ・ジョブ・トレーニングを行うなど、高度SOC人材育成を行います。また、SOC業務を通じて解析者と機械学習エンジンの連携で異種データの横断分析を行い、国産の脅威情報の生成と提供を目指します。

■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長期運用します。そして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・非機能検証を実施します。既存製品との比較や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。

■Co-Nexus C

Co-Nexus C（CYROP）では、ナショナルサイバートレーニングセンターで行っている実践的サイバー防御演習等の演習基盤をCYNEXに応用し、社会的な需要に応じて、システム開発者、経営者、学生向けなどの広範な演習コンテンツを継続して開発し、それを標準的な演習シナリオ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事業の活性化を行います。

■今後の展望

CYNEXは令和5年度のアライアンス本格稼働に向けて現在30を超える初期参画組織と共に各Co-Nexusの立ち上げ、プロジェクト試行を実施しています（図2）。初期参画組織からフィードバックを元にアライアンス運営体制を整え、日本のサイバーセキュリティ結節点を目指します。

＊1　https://www.nisc.go.jp/pdf/council/cs/kenkyu/dai12/12shiryou01.pdf

安心・安全なIoT機器の利用に向けた取組

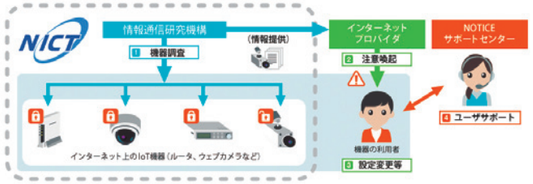


図　NOTICEの取組

井上 大介（いのうえ だいすけ）〈右〉
ナショナルサイバーオブザベーションセンター　研究統括／同センター サイバーオブザベーション運用室　室長
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)。

田沼 知行（たぬま ともゆき）〈左〉
ナショナルサイバーオブザベーションセンター　主管エキスパート／同センター サイバーオブザベーション事業推進室 室長
大学院修了後、1994年郵政省（現・総務省）に入省。通信事業や電波管理に関するルール策定、情報通信分野の研究開発、標準化活動の推進等に従事。2021年から現職。

盛合 志帆（もりあい しほ）
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
大学卒業後、日本電信電話（株）、ソニー（株）を経て、2012年にNICT入所、2021年から現職。暗号、情報セキュリティ、プライバシー に関する研究に従事。博士（工学）。

現在、技術の進展によってあらゆるものがインターネット等のネットワークに接続されるIoT/AI時代が到来し、IoT機器が急速に普及しています。インターネット上のサイバー攻撃では、このIoT機器を狙ったものが急増しており、セキュリティ対策に不備のある機器は悪用されてしまうおそれがあります。ここではこのような環境において安心・安全にIoT機器を利用していただくためにNICTが参加している取組（NOTICE）について紹介します。

■NOTICEとは

NOTICE（National Operation Towards IoT Clean Environment）は、NICTだけではなく、総務省、インターネットプロバイダが連携して行っている取組で、IoT機器へのアクセスを通じてサイバー攻撃に悪用されるおそれのある機器の調査とその機器の利用者への注意喚起を行っています。NICTはサイバー攻撃に悪用されるおそれのある機器の調査と、その調査結果のインターネットプロバイダへの情報提供の役割を担っています。インターネットプロバイダは、その情報を元に該当する機器の利用者に注意喚起を行い、設定の変更等を促しています。総務省は、サポートセンターを設置して、ウェブサイトや電話による機器利用者等からの問合せ対応を行って適切なセキュリティ対策が行えるよう案内しています。この取組は2019年2月から実施しています。取組の全体像は図のとおりです。

NICTでは、この調査・情報提供を行うために2019年1月にナショナルサイバーオブザベーションセンター（National Cyber Observation Center）を設置し、第5期中長期計画開始時からは、サイバーセキュリティ研究所の下で、総務省からの補助金を受けて運営しています。

■調査の実施状況

NICTでは、NOTICEだけでなく、2019年6月からNICTERプロジェクトの一環としてマルウエアに感染してしまった機器に関する注意喚起も行っており、両者の実施状況をウェブサイトで毎月公開しています。2022年5月の実施状況は、

【NOTICEによる注意喚起】
1,564件の対象を検知しISPへ通知
【NICTERによる注意喚起】
1日平均1,025件の対象を検知しISPへ通知

となっています。（詳しくはhttps://notice.go.jp/statusをご覧ください）。調査プログラムの改修、調査対象とするID・パスワード数の追加等、おおむね1年に1回程度調査内容を充実するための対応を行うごとに、注意喚起の対象数が大幅に増えますが、NICTも含めた関係者が協力して着実に取り組んでいることで、対象数は毎月少しずつ減少しています。

■今後の展望

2022年6月からは、調査内容を更に充実させるために調査対象とするプロトコルを追加しました（http/https）。まだ注意喚起に向けた精査等は必要ですが、これによって注意喚起の対象数は更に大幅に増える見込みです。

なお、NOTICEの取組は、上でご説明したとおり政府の全面的なバックアップの下で実施されているもので、NICTは法律（国立研究開発法人情報通信研究機構法：NICT法）に基づいて関係する調査等を実施しており、その実施期間も2023年度末までの約5年間と定められています。これまでの取組状況も踏まえつつ、安心・安全なIoT機器の利用に向けてどのようなことを行っていくべきか、政府や関係機関・企業等を交えた検討が期待される時期を迎えています。

ユーザに寄り添った、真に有用なセキュリティ対策システムの創出に向けて

長谷川 彩子
（はせがわ あやこ）
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
研究員

●経歴

2013年3月	お茶の水女子大学 理学部 情報科学科 卒業
2015年3月	お茶の水女子大学人間文化創成科学研究科 理学専攻 情報科学コース 博士前期課程 修了
2015年4月	日本電信電話株式会社 入社
2021年10月	NICT入所。現職に至る

●受賞歴等
EuroUSEC2021 Best Paper Award
CSS2020最優秀論文賞

一問一答

Q 研究者になってよかったことは？
A 論文採択の喜びを共著者と分かち合えることです。また、自身の研究成果が実際のシステムに反映されたときにはやりがいを感じます。

Q 最近はまっていること
A 最近茶香炉を購入し、茶葉の香りでリフレッシュすることにはまっています。お茶屋さんにいるような気分になれます。

Q 休日の過ごし方は？
A 散歩や家庭菜園の手入れをしています。平日はPCの前にいる時間がどうしても長くなるので、休日はできるだけ自然に触れるよう心がけています。

新しいデバイスやサービスを使い始めるとき、わくわくする気持ちがあるのと同時に、自身のセキュリティ対策が十分であるかという不安を感じる方が多いのではないでしょうか。私自身、セキュリティの研究者でありながらも、1ユーザとしてセキュリティ対策の難しさを感じています。このURLをクリックしてもよいのだろうか、このサービスにおいて自身のデータは安全に保護されているのだろうかなどと悩むこともあります。そのような不安な気持ちがわかるからこそ、ユーザのセキュリティに関する懸念点や課題に寄り添えるような研究者になりたいと感じ、「ユーザブルセキュリティ」と呼ばれる研究分野の研究を始めました。この分野では、ユーザの行動や認識に着目し、ユーザが適切なセキュリティ対策を実施できるようサポートするシステムの実現を目指します。

現在は、ユーザが日常生活の中で抱えているセキュリティ・プライバシーに関する懸念点や課題を明らかにするために、オンラインアンケートやソーシャルメディア分析などの様々な調査を実施しています。困っているユーザが最も多いのは、自身が閲覧したウェブサイトや受信したメッセージが詐欺でないかの判断です。ユーザへの調査を通じて感じることは、ユーザは攻撃者が用いる攻撃テクニックに関する知識をあまり持ち合わせていないということです。例えば、URLのサブドメイン部分に正規のサービス名称の文字列を含めることで正規のサイトであるかのように詐称するといった、攻撃者がよく用いるURL偽装テクニックがいくつかありますが、多くのユーザがそのようなURL偽装テクニックを認識していません。このような状況を踏まえ、ユーザに参照してもらいやすいセキュリティナレッジベースや教育コンテンツを提供することを目指しています。また、デバイスやサービスのセキュリティ設定やプライバシー設定に躓（つまず）いているユーザも非常に多く、現状のデバイスやサービスのデザインがいかにユーザに親切でないかに気付かされます。特に、専門的な技術用語を用いてセキュリティについて説明しているデバイスやサービスが多いことがユーザの混乱を生んでいます。今後は、ユーザが理解しやすい説明方法を探るとともに、デバイスやサービスの提供会社と連携して改善を行いたいと考えています。

これからもユーザに寄り添って懸念点や課題を理解し、ユーザが躓くポイントを一つひとつ解消していくことで、ユーザが安心してデジタル技術を利用できる社会づくりに貢献していきます。

けいはんなR&Dフェア2022

ユニバーサルコミュニケーション研究所

内閣府SIP第二期にてKDDI株式会社、NECソリューションイノベータ株式会社、株式会社日本総合研究所と共同開発

開催日 10月6日(木)・7日(金)

会場 特設Webサイトでのオンライン開催

https://keihanna-fair.jp/

※講演での質疑応答に参加を希望される方は、事前の参加登録が必要です。上記の特設Webサイトにて、氏名やメールアドレス等をご登録ください。

内容

基調講演 10月6日(木) 10:20～11:20

「データ駆動型化学が導く研究・開発・生産のパラダイム変革」

船津 公人 氏
国立大学法人奈良先端科学技術大学院大学
データ駆動型サイエンス創造センター センター長・特任教授
東京大学名誉教授

NICTの主な展示と講演

- (講演) 高齢者の言葉を理解するAIを目指して
- (展示) 誤訳発見技術で翻訳品質を保証する
- (展示) ウクライナ語音声翻訳
- (展示) マルチメディアセンシング
- (展示) リアルで表情豊かな3Dアバターの構築・再現技術「REXR」

ほか、特別講演、技術講演もあります。

けいはんな学研都市内の研究機関や企業、大学、自治体等が協力して、最先端技術の研究成果を基調講演、特別講演、技術講演、研究発表(展示)等でわかりやすくご紹介します。

「電波の日」及び「情報通信月間」は、電波利用又は情報通信の発展に貢献した個人及び団体、デジタルコンテンツの今後の創作活動が期待される者に対して授与されます。

※所属・役職名は受賞者決定時点のものです。

第72回「電波の日」及び 令和4年度「情報通信月間」

Awards for FY2022 Radio Day and Info-communications Promotion Month

第72回「電波の日」 総務大臣表彰

柳田 敏雄
(やなぎだ としお)

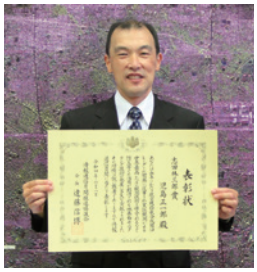
NICTフェロー／未来ICT研究所脳情報通信融合研究センター R＆Dアドバイザー

●受賞日：令和4年6月1日

●受賞内容：国立研究開発法人情報通信研究機構における脳情報通信融合研究センターの設立に尽力するとともに、研究センター長として長年にわたり脳科学とICTが異分野融合した最先端の研究領域である脳情報通信の確立及び発展に多大な貢献 をした。

●受賞の言葉　この度は総務省ご推薦により栄えある賞を受賞し光栄に思います。お世話になった皆様に感謝します。今後はフェロー・R＆Dアドバイザーとして微力ながらCiNetの発展に貢献したいと思います。

令和4年度「情報通信月間」 情報通信月間推進協議会会長表彰「志田林三郎賞」



児島 正一郎
(こじま しょういちろう)

電磁波研究所 リモートセンシング研究室 研究マネージャー

●受賞日：令和4年6月1日

●受賞内容：長年にわたり航空機搭載合成開口レーダーの開発に従事し、実証観測による世界最高レベルの観測技術を確立するなど、防災等での活用が期待される地表面モニタリング技術の発展に多大な貢献をした。

●受賞の言葉　本授賞は、NICT・総務省の関係者やレーダーの製造に携わった方々のお力添えによるところが大きく、感謝申し上げます。私は、今回の栄誉を励みとし、これからもなお一層の研鑽を重ね、世界最高性能のセンサ開発を進めていきます。

令和4年度「情報通信月間」 情報通信月間推進協議会会長表彰「情報通信功績賞」

井上 大介
(いのうえ だいすけ)

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／
ナショナルサイバーオブザベーションセンター サイバーオブザベーション運用室 室長／
サイバーセキュリティネクサス ネクサス長

●受賞日：令和4年6月1日

●受賞内容：国立研究開発法人情報通信研究機構において、長年にわたりサイバーセキュリティに係る研究開発やIoT機器の脆弱性調査など幅広く施策を牽引するとともに、東京2020オリンピック・パラリンピック競技大会において、サイバー攻撃観測体制を整備し通信インフラの安定運営に多大な貢献をした。

●受賞の言葉　栄誉ある賞を頂き大変光栄に存じます。共に研究開発を行う研究者、技術者、解析者、そして支援スタッフの皆様に心より感謝いたします。

その他受賞

◆日本ITU協会「第54回 世界情報社会・電気通信日のつどい」総務大臣賞
イノベーション推進部門 標準化推進室 招聘専門員 **佐藤孝平**

◆2022年度情報通信技術賞（総務大臣表彰）
サイバーセキュリティ研究所 主管研究員 **中尾康二**

◆「第35回独創性を拓く 先端技術大賞」経済産業大臣賞
ユニバーサルコミュニケーション研究所 副研究所長 **鳥澤健太郎**
ユニバーサルコミュニケーション研究所 データ駆動知能システム研究センター 主任研究員 **田仲正弘**

NICT NEWS 2022 No.5 通巻495
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4年（2022年）9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)