国立研究開発法人情報通信研究機構

NICT NEWS

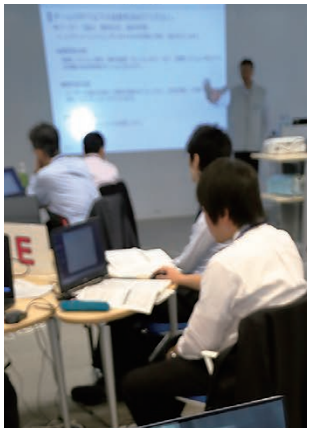
2018
No. 1
通巻 467

FEATURE

爆発的に増え続ける サイバー攻撃から社会を守る

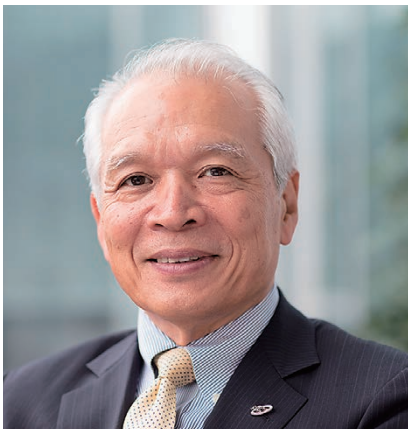
NICT NEWS 2018 No.1 通巻467
国立研究開発法人情報通信研究機構

CONTENTS



表紙写真「若手人材育成事業 SecHack365の集合イベント風景」
写真はトレーニーと呼ばれる参加者が、新しいアイディア創出手法を学んでいる1コマ。この写真のようにPCを使わずに発想法を磨くコンテンツをはじめとして、SecHack365の集合イベントでは、トレーニーの研究・開発を支援するために、様々な工夫を凝らしたコンテンツを用意している（本誌6〜7ページ）。左上写真は実戦的サイバー防御演習CYDERの演習風景（本誌8〜10ページ）。

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

昨年は、米国のトランプ大統領をはじめ、各国で新しいリーダーが誕生しました。また、テロは相変わらず世界各地で頻発し、世界中が緊張感に満ちていました。一方、我々の身近においても、WannaCryによるサイバー攻撃やIoT機器を踏み台にしたMIRAIなどのマルウェアによって、更に大規模化したサイバー攻撃が頻発していました。このような中、IoT・ビッグデータ・AI・サイバーセキュリティ技術等、情報通信分野の技術が大きな注目を集め、それら技術の重要性が強く認識された一年となりました。

NICTは、情報通信分野における我が国で唯一の国立研究開発法人として、ICTの高度化による社会課題の解決や新たな価値の創造を使命とし、その実現のために、日々、世界最先端技術の研究開発へのチャレンジと、その社会展開・実装のためのコラボレーション／オープンイノベーション推進の取組を一体的に進めております。

NICTでは、センシング基盤分野・統合ICT基盤分野・データ利活用基盤分野・サイバーセキュリティ分野・フロンティア研究分野の5分野において情報通信の研究開発を進めるとともに、昨年にはその成果の一層の推進のため、実践的なサイバートレーニングを企画・推進する「ナショナルサイバートレーニングセンター」や、AI分野の研究開発を推進する「知能科学融合研究開発推進センター」を立ち上げました。さらに、自動翻訳システムの様々な分野への対応や高精度化を進めるため、総務省と共同で、関係者の皆様から広くご協力いただきながら様々な分野の翻訳データを集積・活用する「翻訳バンク」の運用を開始しました。また、国内外において、研究機関・企業・大学・地方自治体等と様々な共同研究・実証プロジェクトを進めるとともに、NICTの技術を様々な企業に活用いただく活動や、ITU・IEEE等での国際標準化活動も推進しています。

私は、昨年4月に理事長に就任して以来、コラボレーション、オープンマインド・オープンイノベーション、チャレンジャー精神の3点を運営方針として掲げ、職員にはこれを絶えず意識してもらっています。そして、これらを有機的に連動させ実体化させるための取組として、昨年には機構全体でのオープンな議論を通じて新たな研究テーマの創出等を図るアイデアソンなど、部門間の壁を取り除き様々な意見を吸い上げる試みを進めてきました。また、国内外においてそれぞれの地域における社会的な課題解決に向けた取組を様々な機関とともに推進してきました。また、今後重点的に取り組むべき研究開発課題等についても、一般の皆様から広くご意見を頂くために「ICT分野の更なる発展に向けた意見募集」を行ってまいりました。この取組につきましては本年も継続し、機構の運営に活かす所存です。

NICTでは、幅広く国民の皆様からのご意見も頂き、機構の中に閉じこもることなく、広く関係者の皆様と協力・切磋琢磨させていただきながら産学官連携活動を推進し、引き続きICT分野の更なる発展のために邁進してまいります。今後とも変わらぬご支援、ご協力を頂きますようお願い申し上げます。

最後になりましたが、本年が皆様にとって素晴らしい年になりますよう祈念いたしまして、年頭のご挨拶とさせていただきます。

FEATURE

Protect Society from explosive ever-increasing cyber attack

爆発的に増え続けるサイバー攻撃から社会を守る

INTERVIEW

人材と研究開発コミュニティーのコアな存在をめざして

「サイバー攻撃」の話題がマスコミにも頻繁に取り上げられるようになった今日、その手口の一層の多様化・悪質化も進んでいる。こうした事態に対処するため、これまでのサイバーセキュリティに関する研究開発の知見も活用しつつ、社会に向け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平成29年4月1日付けで設立されたのが、「ナショナルサイバートレーニングセンター」である。その設立の経緯や活動内容について、センター長の園田道夫氏、サイバートレーニング研究室室長の衛藤将史氏、サイバートレーニング事業推進室主任研究技術員の花田智洋氏にお話を伺った。

■サイバーセキュリティ人材が足りない

――まずは、ナショナルサイバートレーニングセンター設立の経緯について教えていただけますか。

衛藤　2011年、大手企業が大規模なサイバー攻撃を受ける事件が大きなニュースとなりましたが、以後、2010年代前半に大手企業が標的となった情報漏洩事例が立て続けに起こっています。これら事件を背景とした危機感の高まりを受け、社会的にセキュリティを担う人材の不足が指摘されるようになりました。これに関して、経済産業省では、2020年までに19.3万人の人材が不足するであろうという報告書も出されています（『IT人材の最新動向と将来推計に関する調査結果～ 報告書概要版 ～』平成28年6月10日）。

こうした背景があって、内閣サイバーセキュリティセンター（NISC）が中心となり、政府でもセキュリティ人材の育成に力を入れていこうという機運が高まってきました。その具体的な動きとして総務省で平成25年度から始まったセキュリティ人材育成のプロジェクトが、現在、我々ナショナルサイバートレーニングセンターが担う事業の一つとなっているサイバー防御演習「CYDER（サイダー）」です。つまり、当センター発足以前にCYDERは始まっていたわけです。

CYDERが良好な成果を上げてきたことで、さらに規模を拡大するとともに新たな知見、技術を加えて内容を深めたいという意向が、出てきました。一方で、東京2020オリンピック・パラリンピック競技大会（以下「東京2020大会」）開催が決定、その適切な運営のためにもセキュリティ人材の育成はさらに急務となりました。こうした経緯から、以前よりサイバーセキュリティの研究に取り組み、深い知見を持つNICTにCYDERの事業を引き継ぐとともに、東京2020大会に向けセキュリティ対策の強化を目的に、NICT内に新組織を立ち上げることになったのです。

第一段階として、平成28年度にセキュリティ人材育成研究センターを発足。これを前身として人員を拡充・改組し、平成29年4月、ナショナルサイバートレーニングセンターが設立されました。事業としては、総務省から移管された実践的サイバー防御演習CYDER、東京2020大会に向けた実践的サイバー演習である「CYBER（サイバー）COLOSSEO（コロッセオ）」の2つに加えて、センター発足後、より将来を見据えた若手人材の育成を目指した「SecHack365（セックハックサンロクゴ）」を新規プログラムとして立ち上げています。この3つが柱となっています。

■仮想ネットワーク上でサイバー攻撃を体験するCYDER

――1本目の柱、サイバー攻撃防御演習CYDERの内容や実施状況などをお聞かせください。

園田　近年、サイバー攻撃による被害が様々な組織で起きています。サイバー攻撃に対しては、攻撃を受けた直後から適切に対応しなければ、組織の被害は急速に拡大してしまいます。被害を完全に防ぐことは難しいとしても、その拡大を防ぐために、いかに適切な判断を下し、行動するか。被

左から衛藤、園田、花田（プロフィール5ページ参照）

害を最小限に抑えるには事件初期の対応が重要になってきます。そうした初動対応のトレーニングを行うのがCYDERです。

例えば災害現場において多数の負傷者が出た場合、医療スタッフは手当の緊急度に従い優先順を付けます。これを「トリアージ」と呼ぶのですが、セキュリティにおいても同様のことが必要で、特に事件対応（インシデント・レスポンス）においては、重篤な部分に優先的に対処することが必要になります。では、重篤な部分はどこに潜んでいて、どんな事象として表れているのか。また、その次の段階として、関係する組織とどのように調整すべきなのか。短期間のうちに判断を下し、行動しなければいけません。CYDERではそれらをシミュレーションし、トレーニングを行うのです。

CYDERの受講者には、まず、1時間程度の「事前オンライン学習」を受けてもらいます。その後、実際に会場に集まり、1日がかりで演習を行います。1チーム3名～4名程度でチームを組んでもらい、1回の演習には約10チームが参加します。 NICTは「StarBED（スターベッド）」という大規模計算環境を保有していますが、このStarBED上に10チーム分の仮想端末で構成される仮想的なネットワークを構築。各チームは、その仮想ネットワークを舞台にサイバー攻撃や対処方法を体験・学習します。

コンピュータのログを見て怪しいデータを探し、どこに感染源があるかを特定し、封じ込めを試みる。さらには特定に至る分析や対処が適切かどうかをディスカッションし、最終的には、「こうした事態が自分の組織に起きた場合にどうしたらいいのか」を考え、そうした知識や体験を持って帰っていただく。それが、CYDERの一連の流れです。

CYDERの受講者は総務省時代には年間200名規模でしたが、NICTに移管したタイミングで1,500名まで拡大。平成29年度はさらにその倍で3,000名の規模で実施しています。また受講対象も、当初はほぼ中央省庁のみでしたが、地方自治体や独立行政法人などにも拡大。実施会場も昨年までは11拠点でしたが、今年度は47都道府県で行っています。

最近では省庁や自治体以外の方々からCYDERをぜひ実施してほしいという要望もあり、有償でのCYDERの演習メニュー提供も開始しています。規模が小さくセキュリティ担当者が1名といった組織であっても、そうしたところが集まって申し込むことで、受講していただくことが可能です。

■より深く実践的なCYBER COLOSSEO、将来を見据えたSecHack365

――2本目の柱、CYBER COLOSSEOは東京2020大会に備えて、ということで、より具体性が高いですね。

衛藤　CYDERは中央省庁や自治体の担当者の方を対象に、いわば全体的に広くセキュリティ・レベルの底上げを図るというコンセプトですが、CYBER COLOSSEOは東京オリンピック・パラリンピック競技大会組織委員会等のセキュリティ関係者を集中的に育成するというのが大きな目標です。これも平成28年度に開始、初回は総務省が実施し、2回目以降NICTに移管されています。

INTERVIEW

人材と研究開発コミュニティーのコアな存在をめざして

東京2020大会という具体的な目標があり、CYDERよりも深いレベルでの育成を目指す必要があるため、防御をメインに学ぶCYDERに対し、CYBER COLOSSEOでは攻防戦形式でのシミュレーションを行うのが大きな特徴です。攻撃者の意図を理解することで、より効果的な防御を行えるようにするわけです。

東京2020大会は世界的に注目を集めるイベントであるため、サイバー攻撃も大量に押し寄せてきます。実際、2012年のロンドン・オリンピックの際は、チケットサイトが攻撃によりダウンする事態が発生しています。障害の規模や種類によっては収益に影響するだけでなく、その大会のブランドが大きく損なわれる可能性もあります。当然ながら、国や東京都でもいかに運営やサービスをスムーズに動かすかに神経を注いでいますし、NICTとしても、東京オリンピック・パラリンピック競技大会組織委員会等と緊密に連携しつつ、よりよいプログラム構築に努めているところです。

――SecHack365はセンター発足後の新たなプロジェクトでもあり、前2者とはだいぶ趣も違うようですが、どのような内容なのでしょうか。

花田　SecHack365は、単に既製品のソフトウェアを「運用」するだけでなく、自ら「研究・開発」していける若手イノベーターの育成を目指したもので、25歳以下のトレーニー（受講者）を一般公募で集めています。平成29年度のトレーニーは、下は10歳の小学生から、上は社会人まで、幅広い構成になっています。選考は応募課題への回答内容、熱意や希望などに基づき、個人情報を伏せて行ったのですが、その結果、意図せずにそれだけ年齢層に幅が出ました。

SecHack365では、彼らトレーニーに対し平成29年度末まで接していきます。具体的にはオンラインでの開発環境やコミュニケーション基盤を用意、おおよそ2カ月に1度は集合イベントとして主に合宿形式でのハッカソン*などを実施するほか、各人が開発した内容の発表イベント、先端企業の見学会なども行っていきます。

通常のハッカソンは運営側が単一のテーマや方向性を定めて開催されることが多いのですが、SecHack365では、各トレーニーが作りたいもの、研究したいものを自分の興味に従って決め、それをトレーナーである実施協議会メンバーが継続して支援して

SecHack365　2017年8月23日～25日（福岡回）の様子


左右写真：CYDER 演習2017年6月20日（総務省講堂）の様子

いくというのが大きな特長です。実際に、かなりバリエーション豊かなテーマが出ています。それを支えるトレーナーの層の厚さもSecHack365の強みであるため、トレーナー人材は今後もますます増やしていく方針です。SecHack365の365は、1年間（365日）を指していますが、これは、1年間にわたって、こうした濃密な環境で意欲のある人材に学んでもらったら、どれだけのものができるだろうか、という挑戦でもあるのです。

■セキュリティを担う、大きく緩やかな枠組みのコアに

――間近に迫る東京2020大会への対処から、より将来に備えた人材の育成まで、興味深い事業を行っているセンターですが、今後の方向性や抱負についてもお聞かせください。

園田　ナショナルサイバートレーニングセンターは、「更に広がって行かなければいけない組織」だと思っています。それは単純に事業を拡大するというだけではありません。サイバー攻撃を防御できる人材、セキュリティに関わる人材を育成し、技術やノウハウを伝えるといっても、現時点ではカバーし切れていないところもあります。では、カバーするにはどうしたらよいのか。

「来ていただくことができないなら、人を派遣する」といった「人材と費用負担で解決」以外にも、例えば、来ていただけなくても提供できる仕組みを作ろうとか、いろいろと工夫の余地があると思うのです。当センターならでは、NICTならではのそうした工夫できる環境やきっかけを、今後さらに増やしていきたいというのがひとつ。

さらに、SecHack365の実施協議会メンバーもそうですが、センターの内外に関わらず、コミットする度合いは様々でも、事業に参加していただける多くの方々が連携していく仕組みを作っていきたい。それはそれぞれの研究・開発を深める基盤にもなるし、緊急時に協力し合える体制作りにもなります。そうした基盤のコアとして、我々のセンターが機能するようになればと思っています。

＊ハッカソン：ソフトウェア・エンジニアリングを指すハック（hack）とマラソン（marathon）を組み合わせた造語。主にソフトウェア開発分野でのイベントで、プログラマーやエンジニアが集まり、集中的に開発を行う。

園田 道夫（そのだ みちお）
ナショナルサイバートレーニングセンター
センター長

大学院工学博士課程修了。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。

衛藤 将史（えとう まさし）
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

2005年NICT入所。以降、2016年までサイバーセキュリティ研究室 研究員。2016年より現職。ネットワーク運用管理技術、アプリケーショントレースバック技術、NICTER プロジェクト、IPv6セキュリティ、ITS セキュリティなどサイバーセキュリティ関連技術の研究開発、国際標準化、人材育成に取り組む。博士（工学）。

花田 智洋（はなだ ともひろ）
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
主任研究技術員

2017年NICT入所。前職では銀行基幹系システムの開発にプロジェクトマネージャーとして携わり、本業以外の活動として、九州で情報セキュリティコミュニティを立ち上げ、勉強会やイベント等を主催。現在は主任研究技術員として、ナショナルサイバートレーニングセンター3大事業のCYDER, CYBER COLOSSEO, SecHack365に携わる。

SecHack365 https://sechack365.nict.go.jp/

1年にわたる若手人材育成事業SecHack365

実施協議会委員手作りのSecHack365ロゴ

佐藤 公信（さとう ひろのぶ）
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
主任研究員
高知工科大学客員研究員
SECCON実行委員
セキュリティ・キャンプ講師
SEC道後プログラム検討会委員
SecHack365実施協議会委員

2008年大学院博士後期課程修了後、大学総合研究所助教。2009年高知工科大学地域連携機構助教、2012年工業高等専門学校電気情報工学科助教、2016年工業高等専門学校ソーシャルデザイン学科准教授。ニューラルネットワークを用いたアプリケーションの開発に従事。2016年NICT入所。博士（工学）。

SecHack365（セックハックサンロクゴ）はSecurity（セキュリティ）とHackathon（ハッカソン）からなるかばん語（混成語）で、高度な技術力を持つ研究者や開発者育成により、日本のセキュリティ技術力、産業競争力向上を目的として、平成29年度から開始されたプログラムの名称です。

日本発セキュリティ製品の世界的なシェアは、決して大きいものではなく、どのようなアルゴリズムで動作しているか、細部まではっきりと分からない海外製品を導入せざるを得ないのが現状です。このような状況を打破すべく、また、未来のサイバーセキュリティ研究者・起業家を輩出するために、25歳以下の若手に対して、研究・技術開発を指導するプログラムとしてSecHack365は企画されました。

■プログラムの概要

SecHack365は、次のような内容で構成されています。

- **ハッカソン**
  技術者らが一定時間会場に詰めてソフトウェアなどのアイディアや成果を競い合うイベントのことで、セキュリティやソフトウェア開発等各分野で活躍する実施協議会委員のサポートの下、最先端のセキュリティ関連技術の研究・開発を体験
- **遠隔開発実習**
  NICTが用意したセキュリティ向け遠隔開発環境『NONSTOP』に自宅等からVPN[*1]経由で環境に接続して研究・開発を継続
- **コンテスト演習**
  特定の技術領域に偏らず、参加者それぞれの能力を活かすことのできるコンテストを実施
- **最先端の研究データの活用**
  長年にわたるNICTのサイバーセキュリティ研究によって得られた、膨大かつ貴重なセキュリティ関連データを活用

初年度は358名の応募があり、応募書類を基に熱意と発想力を観点として 47名の

SecHack365のプログラム概要

図1　2017年6月蒲田（東京）回コンテンツ

テーマ	アイディア脳になろう!
目的	創造力刺激
会場	富士通PLY（富士通株式会社）
トレーナー＆ゲスト	富士通株式会社／佳山こうせつさん、 武田英裕さん 株式会社イッツ／久保田達也さん

・会場には3Dプリンターといった発想を刺激するものが多くあり、これらを生かしながらトレーニーのみなさんが、アイディア脳をフル活用、アイディア創出に取り組んだ
・視点や距離を変えアイディアを創り出すといった、変化の激しい現代に必要な，新しいアイディア創出手法について学ぶ機会をご提供いただいた

図2　2017年8月福岡回コンテンツ

テーマ	アイディアから「物づくり」へギアチェンジ!
目的	コラボで物づくり
会場	LINE福岡株式会社　休暇村志賀島
トレーナー＆ゲスト	LINE株式会社／愛甲健二さん

・トレーニーがこれまでに創出したアイディアを、他のトレーニーやトレーナーに発表し、フィードバックを得て作品をブラッシュアップする場である「アイディア見本市」を実施
・マルチトラックのハンズオン演習「縁日」を実施。RaspberryPi*2を利用したルーター自作、深層学習に触れる、ひたすらはんだ付けする"はんだ付け1000本ノック"といった屋台が出店

参加者（トレーニー）を選抜しました。トレーニーが会場施設や会場周辺環境、企業見学やゲストハッカーといった、環境や人々から刺激を受けて自由な発想やトレーニー同士の活発なコラボレーションを生み出だせるように、開催地を東京、福岡、北海道、大阪、沖縄と、様々な地域に設定しました。

SecHack365の運営にあたっては、当機構及び外部のセキュリティ専門家の方々からなる『SecHack365実施協議会』を組織しています。実施協議会委員は、トレーナーとして技術的サポートをしていただいています。これ以外にも、会場、実施協議会委員、トレーニー所属校、ご家族のみなさまを含め、多くの方々のご支援を頂き、SecHack365の実施に至っているものです。

また昨今、セキュリティに関する知識はあるものの倫理や法制度までは理解していない若年層による、ウィルス作成罪での補導がメディアで取り上げられています。SecHack365では、「研究倫理」「サイバーセキュリティに関わる実際の法律」「守られるルール、守られないルール」といった題材をテーマとして、ハッカソンによる研究技術開発だけではなく、セキュリティに関わる倫理や法制度教育についても実施しています。

■SecHack365だからできることを

SecHack365では、同じ目的や価値を共有するトレーニーの集まりを、コラボ（レーション）と呼んでいます。もちろん単独開発もOKですが、アイディア見本市等を通して「コラボ」をみつけても構いません。卒業研究のテーマ、学んできたことや社会経験といったバックグラウンドの違う人との相乗効果により、独りでは発想・開発し得なかった技術追求が可能となります。

特に福岡回では、トレーナーの専門分野の技術や知見をトレーニーに提供したいという思いから、縁日が実施されました。

アイディア見本市や縁日（図2参照）でのインスピレーションと、玄界灘の絶景に面した環境の良さが相まって、福岡回後半はハッカソンに熱が入っていました。終了後もSNS上のコミュニケーションは活発で、ハッカソン熱を日常生活においても保てているようです。

■成果発表会に向けて

1年間にわたるプロジェクトのSecHack365ですが、3月の成果発表会が間近となり、初めてのSecHack365の終わりがもうそこまでやってきました。私自身、トレーニーから創出される、自分とは異なる視点でのアイディアで刺激を受け、学ぶことが多い1年でもありました。

最後になりますが、今後のトレーニーのみなさんのご活躍と、次年度新たなトレーニーのみなさんとの出会いやコラボレーションを楽しみにしています。

＊1　VPN（Virtual Private Network/仮想プライベートネットワーク）
インターネット上などで暗号化した通信を行うことによって、安全に通信を行う技術
＊2　RaspberryPi（ラズベリーパイ）
ラズベリーパイ財団により開発された教育用のコンピュータ

CYDER Cyber Defense Exercise with Recurrence　*http://cyder.nict.go.jp/*

実践的サイバー防御演習事業（CYDER：CYber Defense Exercise with Recurrence）の推進

島田 弘一（しまだ こういち）
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
室長
1980年郵政省電波研究所（現NICT）入所。

川里 真奈（かわさと まな）
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
主任
2009年NICT入所。

近年、サイバー攻撃の手口は巧妙化かつ多様化し、国の行政機関、地方公共団体、重要インフラ等に対する攻撃は増加の一途をたどっています。その対策として、様々なサイバーセキュリティ製品やサービス等の導入が進められていますが、それだけでは十分とは言えず、サイバー攻撃を未然に防ぐことは非常に困難となっています。それどころか、長期間侵入されていることに気づかない組織も数多く存在すると言われています。

100%防げないのであれば、万が一、自組織がサイバー攻撃を受けた際、適切な対処ができるような訓練を、予め受けておくことが重要になります。

NICTでは、サイバー攻撃を受けた際に取るべき一連の対処行動を、実践的に演習するプログラム『CYDER（サイダー）』の実施を通じて、情報システム管理者等のインシデントレスポンス能力の向上を図っています。これにより、ベンダ任せではなく、日常のシステム運用等を考慮しながら、事業継続を脅かす攻撃に対処することができる「総合力の高い情報システム管理者」の養成を目指しています。

■CYDERの沿革

CYDERは平成25年度から平成27年度まで総務省の実証実験として実施されてきた演習プログラムです。本プログラムに対して、NICTでは北陸StarBED技術センターに構築されている、大規模演習環境を提供していましたが、平成27年9月に閣議決

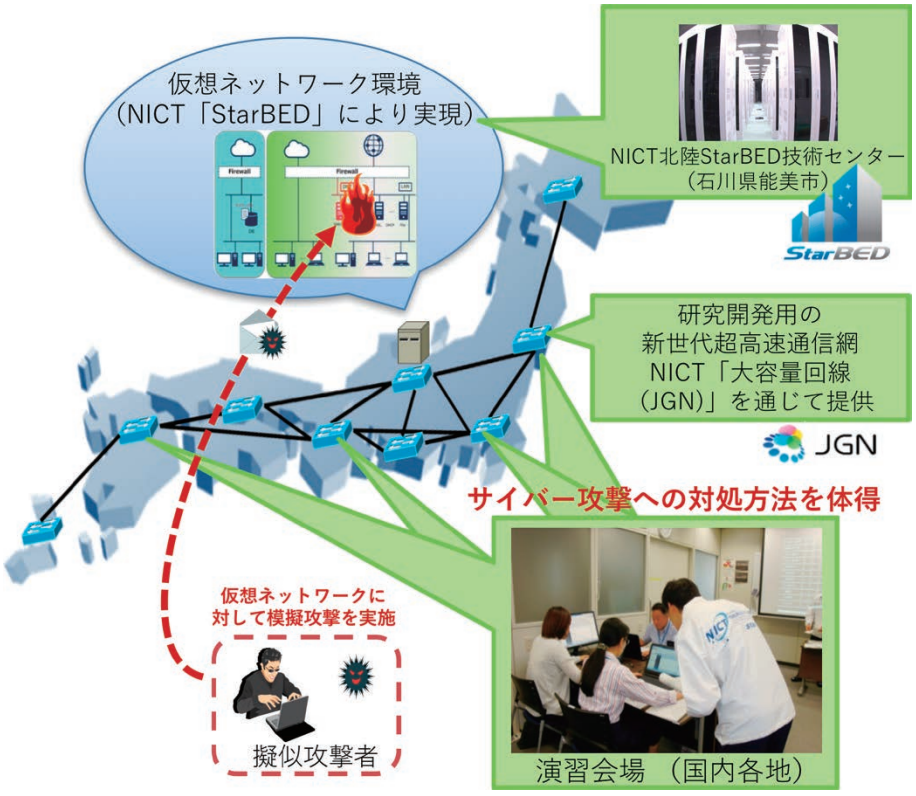


図1　CYDERの演習イメージ

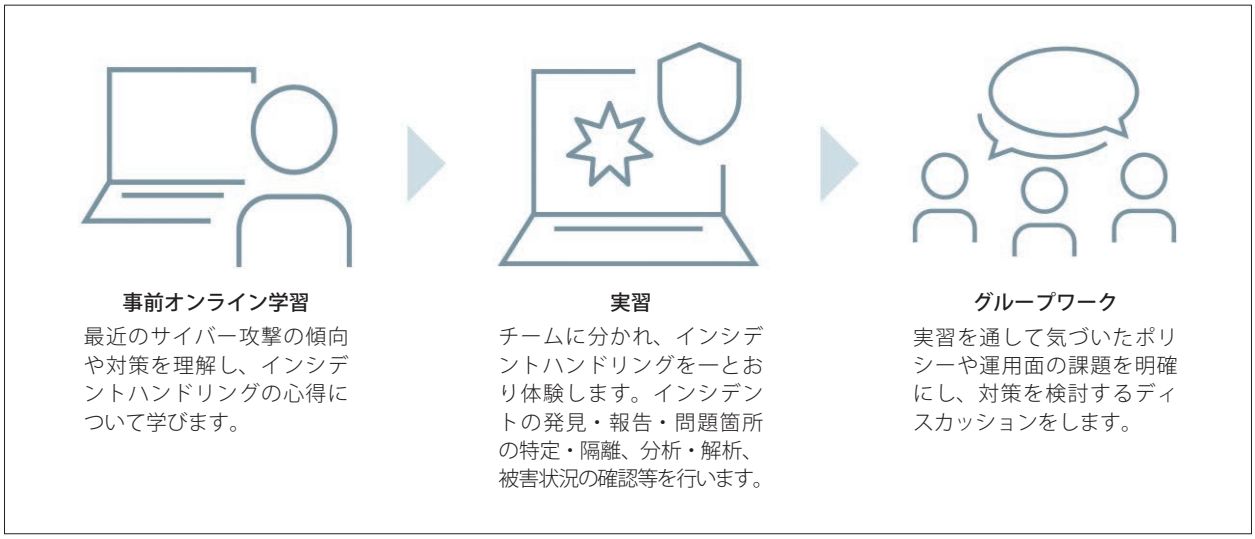


図2　CYDERのカリキュラム

定されたサイバーセキュリティ戦略により、行政機関や重要インフラ等における実践的な演習・訓練のため、NICTが有する演習基盤や攻撃観測・分析に対する技術的知見を活用することになりました。翌、平成28年5月には情報通信研究機構法改正によってCYDERの事業主体がNICTに変更され、これにより、安定的かつ継続的な運用を可能にするとともに、演習実施体制の大幅な強化を図ることとなりました。

■CYDERの概要・特徴

CYDERの最大の特徴は、NICTが長年にわたり蓄積したデータに基づき、サイバーセキュリティ、サイバー攻撃に係る我が国固有の傾向等を徹底的に分析し、現実のサイバー攻撃事例を再現した最新の演習シナリオを用意していることです。このシナリオを基に、国の行政機関、地方公共団体、重要インフラ等の情報システム担当者を対象に、受講者が3～4人1チームとなって演習を行います。

具体的には、NICTの北陸StarBED技術センターに設置された大規模高性能サーバー群を活用して組織のネットワークを模擬した環境を作り出し、そこに最新のサイバー攻撃を擬似的に発生させ、インシデントの検知から対応、報告といった一連の対応を実習していただきます。これらは、実際の機器やソフトウェアの操作を伴って進められます。

■CYDERのカリキュラムについて

まず、受講者は実習受講前にオンライン学習を行っていただきます。この学習をとおして、セキュリティに関する基礎的な知識や演習に必要な知識を学ぶことができます。

実習では、PCの画面を見ながら自身で実際に操作を行うことで、実作業を身に着けることができます。

実習後のグループワークでは、まず各チームでリーダーと書記を決め、実習をとおして気づいた運用面等の課題や対策について検討する議論を行ったり、他チームに対してグループ発表を行ったりします。また、受講前と後にチェックテストを行うことで、どのくらい知識が身についたのかを確認することができます。

これら一連の作業で、受講者が所属組織に戻った後は、すぐに実務に活かすことができるでしょう。また、受講生のスキルレベルや進捗状況に応じたサポート体制も整っているので、セキュリティ初心者でも受講が可能です。

■CYDER実施状況

平成28年度は全国11地域において39回開催し765組織、1,539名が受講しましたが、受講枠を大きく上回る申込希望があったため、やむを得ず人数制限を実施しました。

その経緯を踏まえ、平成29年度は開催規模を大幅に拡充し、全国47都道府県において計100回3,000人以上の受講数を目標としています。

今年度は平成29年6月20日に総務省講堂にて当センターの開講式典を行い、式典に併せて今年度のCYDER（1回目）を開催し、47都道府県で順次実施しています。

■今後のCYDER

2020年の東京オリンピック・パラリンピックの開催が近づくにつれて、サイバー攻撃はますます悪質化し、巧妙化していくことが予想されます。

悪質化していくサイバーテロに対抗するため、CYDER演習を通じてサイバー攻撃に耐え得るサイバーセキュリティ人材を育成していくことが急務であると考えています。

COLUMN

CYDERの演習内容とその裏側

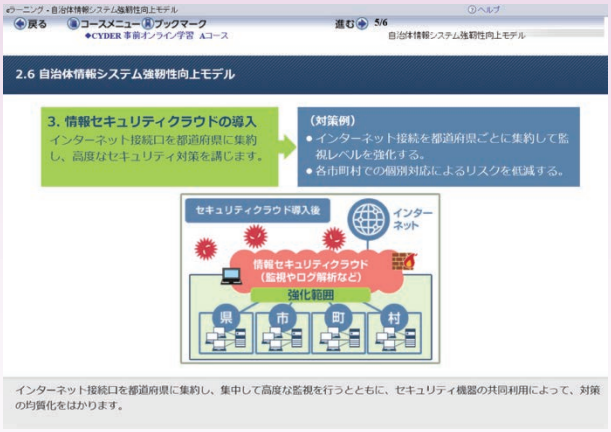
今年度のCYDERは「事前オンライン学習」「実習」「グループワーク」の3つから構成されますが、ここでは、その演習内容や裏側にある環境の一部を紹介します。

金濱 信裕（かなはま のぶひろ）
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
主任研究技術員

■オンライン事前学習

CYDERのオンライン事前学習はLMS（Learning Management System）上に構築され、一般的なe-Learningと同様、誰でも簡単に受講ができる仕組みにしています。またこれらは、全国各地にいる受講者に配慮するため、Webブラウザを利用してインターネット経由で全国どこからでもアクセス可能な環境を北陸StarBED技術センター内に構築しています。

また通常、業務で忙しい受講者の皆様に対し、できる限り負担を少なくするため、コンテンツ全体を実習のインシデントハンドリングに必要な最低限の予備知識等をコンパクトにまとめて、60〜90分程度で完了できる程度のボリュームに絞り込んでいます。さらに、細かく章立て、項目立てを行い、イラスト等も多用することで、ちょっとした業務の合間を使って、飽きずに少しずつでも受講できるように、1項目当たりの受講目安を3〜5分程度にするなどの工夫も取り入れています。



事前オンライン学習画面

■実習・グループワーク

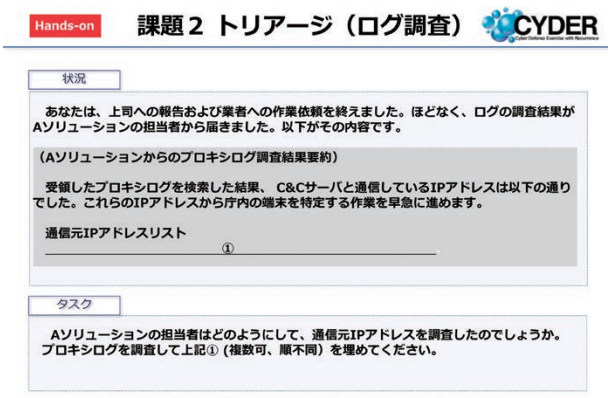
CYDERの中心となる集合演習は、1チーム3〜4名ごとのグループで行います。シナリオに沿ってインシデントハンドリングの手順1つひとつを「課題」や「マイルストン」として、「検知・連絡受付」から「封じ込め」や「報告書作成」に至る一連の作業を実際の機器やソフトウェアの操作を行いながら実践的に体験していただきます。

マルウェアに感染し不正な通信を行っている端末をProxyサーバ等のログから特定するといった、実際の現場で役立つ内容を数多く盛り込んでいます。また演習のシナリオについては、NICTのサイバーセキュリティ研究所が持つ最新かつ高度な知見を取り入れ、毎年新しいシナリオを作成しています。例えば、今年度のBコースのシナリオは、今年世間を賑わせたWannaCryの事案やApache Struts2でも利用された、アプリケーションの脆弱性をねらう攻撃手法を想定した内容にしています。

演習環境はLMSと同様にStarBED内に構築しており、チームごとに、実際の組織内にあるネットワークを模して構成しています。

また、最後のグループワークでは、これらの対応を自身の組織、環境、セキュリティポリシー等に置き換えた場合にどのように対処するか？といった視点で議論をしていただいています。

このようにCYDERは演習全体を通して、ここで得られた実践的な体験を自組織に持ち帰り、それらを実際の現場で活かしていただくことに重点を置いた内容となっています。

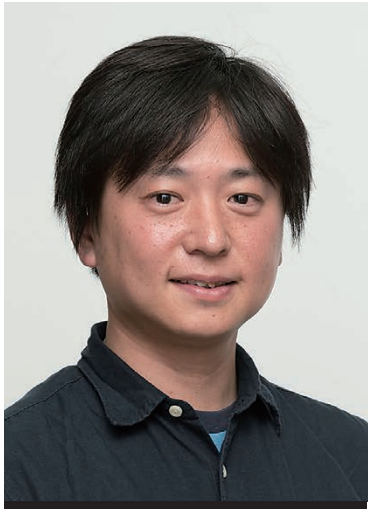


課題・マイルストン例

cyber colosseo　https://colosseo.nict.go.jp

サイバーコロッセオ事業紹介

東京 2020 オリンピック・パラリンピック競技大会の安定的な運営に向けて



衛藤 将史（えとう まさし）
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

2020年に『東京2020オリンピック・パラリンピック競技大会（以下「東京2020大会」）』が開催予定ですが、このような全世界から注目される国際的かつ大規模なイベントは、攻撃者にとって格好のサイバー攻撃の対象となることが予想されます。サイバー攻撃によるイベントの中止や関連業務の継続が妨げられることなく、適切に運営が維持されるよう、通常の業務に加え、サイバーセキュリティに関するノウハウの蓄積と人員強化が急務となっています。

情報通信研究機構（NICT）が実施するサイバーコロッセオ（CYBER COLOSSEO）は、東京2020大会の安定的な運営に向け、同大会関連組織のセキュリティ関係者を対象に行われるサイバー演習です。

サイバーコロッセオでは大会開催時を想定した模擬環境上で、攻撃・防御技術の双方に関する実践的な講義演習と攻防戦を主体とする実機演習を通じて、CYDER 演習相当の技術レベルに加え、より一段階上のレベルの人材育成にも取り組みます。

サイバーコロッセオの演習は東京2020大会の関係団体のうち、大会組織委員会の各部門とその担当システムベンダの職員を対象として実施されます。また演習のレベルは下の表に示すとおり初級から準上級まで用意されており、受講者は自身の技術力に合わせて受講内容を決めることができます。

初級から準上級までの各コースは、技術実習を含む実践的なサイバーセキュリティ技術に関する座学と実機演習によって構成されています。特に準上級コースではWeb、ネットワーク、フォレンジクス等、受講者の技術領域に特化した形での攻防戦を予定しています。

以上のとおりサイバーコロッセオは、受講者の技術レベルや技術領域に応じた様々な教育コンテンツを用意し、攻防戦形式の演習を繰り返すことで受講者の能力向上を図る演習プログラムです。

本イベントは、今年度の開催を皮切りに2020年の大会本番に向けて継続的に実施され、関係組織のサイバー攻撃対応力の事前強化に取り組む予定です。

	各コース受講時にあらかじめ必要な知識	受講対象者（育成したい人物像）
初級コース	・コンピュータ（特にWindows）に関する操作経験	・ユーザとしてのPC/NW 利用者で今後セキュリティ管理業務に従事する人
中級コース	・コンピュータとネットワーク（特にWindowsとTCP/IP）に関する基礎知識 ・サイバーセキュリティに関する基礎知識	・セキュリティ管理業務を主導する立場の人 ・インシデント対応にあたってユーザや内外関係部門との連絡調整役を担う人
準上級コース	・コンピュータとネットワーク（特にWindows, Linux/Unix, TCP/IP）に関する知識 ・サイバーセキュリティ（特にネットワークセキュリティ、バイナリ解析、フォレンジクス、ウェブセキュリティ、データベースセキュリティ、OS セキュリティ、ストラテジー／ガバナンスのいずれか）に関する知識	・高度なサイバー攻撃に対して自身の力で即時的に対処できる人 ・マルウェア検体や感染端末の詳細な解析技術を有する人

表　サイバーコロッセオのコース設定

※ 準上級よりも高度な技量を必要とする、いわゆる「上級」レベルの人材は、訓練での育成ではなく、セキュリティソリューションを提供するベンダ等から十分に実務経験を積んだ人材を登用することが望ましいため、本事業では初級・中級・準上級の人材育成に特化して取り組んでいます。

広帯域の電磁波で観たフラアンジェリコの壁画

電磁波研究所電磁波応用総合研究室 室長　福永 香

技術も美術も人間による創造という点で同じArtとして扱われていたルネッサンス時代に描かれ、私たちが鑑賞している美術作品のほとんどは、物体として存在し続けるための様々な修復処置が施されてきました。1970年代以降は美術史的な興味及び修復前の状態把握を目的として科学的な調査が積極的に行われるようになり、電磁波を用いた観測は非破壊非接触で内部構造や材料の情報を得られるため広く用いられています。

2016年度、西暦1442年頃に画僧フラアンジェリコによりブオンフレスコ技法で描かれた「受胎告知」の調査をフィレンツェの応用物理研究所とともに行いました。聖母マリアに大天使ガブリエルが受胎を知らせに来る場面で、ルネッサンス期の主要なテーマです。この作品は日本人観光客も多く訪れるイタリア・フィレンツェの元修道院のサンマルコ美術館2階にあります。

調査は目視から始まりますが、デジタル撮影技術の進歩により、ルーペを使うレベルの微細な部分まで観察できるようになりました。今回は、横幅3.2m、高さ2.3mの壁画を1000ppiの解像度で、休館日の8時間以内で撮影するため、3台のカメラで同時に連続自動撮影できる（株）日立製作所のシステムを用いました。図1は可視画像と、その中で尖った部分を抜き出すような処理をした白黒画像を比較したもので、通常の鑑賞状態では見えにくいひび割れがよくわかります。

可視光領域より広い帯域の電磁波を用いると、壁内部から下地、描画層に至るまでの構造や、顔料の種類、過去の修復材料等がわかります。図2は、テラヘルツ波で壁画内部を観察しながら、蛍光X 線装置で壁画上部の元素分析をしている様子です。ただし、それぞれの装置から得られるデータは限られた情報しか持たないので、全てを比較し、さらに絵画技法、美術史的知見を総動員して診断することが重要です。例えば、図1で、ひび割れの多い部分とそうでない部分は、フレスコ画特有の事情である「1日で彩色する範囲だけの絵画用の層（ジョルナータ）を当日つくり、継ぎ足しながら描く」ことから、ジョルナータの出来がクラックに影響したという推論を引き出せます。マイクロ波やテラヘルツ波を用いると、ジョルナータと下地との界面に不連続面があることを確かめられ、さらに赤外線から紫外線の領域を用いた材料調査で、再固着させる修復処理がされていたことがわかる、という具合です。

図1　高精細で撮影した画像でひび割れを見やすくする処理をした例

今回の調査で得られた成果は、Sillabe 社より書籍として出版されました。また、得られた高精細画像や科学調査データを用いたデジタルミュージアムイベントの開催を予定しています。NICTが世界に先駆けて成功した、絵画層と下地の界面の解析技術は、エストニア共和国タリン市からの要請で、複数の作品の技法解明に用いられるなど、広く活用されています。

図2　電磁波を用いた科学調査中の様子。壁画下方に衝突防止用ガラス板があり、そこにエアキャップを掛けている。左中央の自動計測中の装置は、パイオニア（株）製のテラヘルツ波イメージャー。右上がハンディタイプの蛍光X線装置で元素分析中の筆者

福永 香（ふくなが かおり）

大学院修了後、株式会社フジクラ勤務を経て1994年に郵政省通信総合研究所（現NICT）に入所。電磁波を用いた非破壊検査の研究に従事。日本学術会議連携会員。博士（工学）、学士（造形）。

Awards

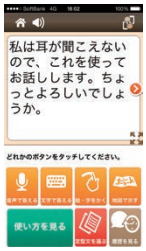
「産学官連携功労者表彰」は、企業、大学、公的研究機関等の産学官連携活動において大きな成果を収め、また、先導的な取組を行う等、産学官連携活動の推進に多大な貢献をした優れた成功事例に対して贈られる賞です。「Red Hat Innovation Awards」は、オープンソースを活用したITの課題解決、情報テクノロジーの変革／モダナイゼーションによるイノベーションの促進及びアジリティや生産性の向上を達成した企業に授与されます。

内閣府
第15回産学官連携功労者表彰 総務大臣賞

Minister for Internal Affairs and Communications Award

葦苅　豊（あしかり ゆたか）

先進的音声翻訳研究開発推進センター
統合システム開発室 室長



聴覚障害者は文字で質問を入力し音声で相手に伝えます。健聴者は音声で答えるだけで文字になって相手に伝わります。

概要

●受賞内容：スマホ等用のアプリ、「こえとら」の開発と展開に係る産学官連携により、共生社会の実現に大きく貢献したことが評価され、受賞しました。「こえとら」は、NICT の開発成果である音声認識・合成技術を活用して音声と文字を相互にリアルタイムで変換し、聴覚障害者等と健聴者との間の円滑なコミュニケーションを支援するものです。平成27年1月に株式会社フィートに技術移転され、現在、52,152回ダウンロードされています（2017年10月31日時点）。

●共同受賞者：小林照二(株式会社フィート)、有木節二(一般社団法人電気通信事業者協会)

●受賞日：2017年8月21日

受賞の言葉

熊本ろう学校の山田先生から頂いた一通のメールをきっかけに聴覚障害者等支援アプリ「こえとら」を開発しました。

このアプリの有用性が評価されて民間企業に技術移転することができ、永続的な運用を行っていただいております。全てはNICTの音声翻訳研究の賜であり、研究者の皆様方ならびに山田先生に深く感謝いたします。今後も社会の役に立つシステムの開発に邁進していきたいと思っております。

Red Hat Innovation Awards APAC 2017
カテゴリー：ITの最適化／クラウド・インフラストラクチャ

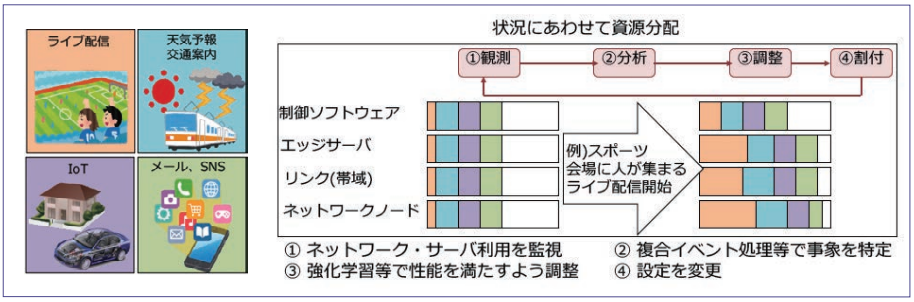
国立研究開発法人情報通信研究機構*

＊組織として受賞

概要

●受賞内容：NICTが提唱する網・計算資源自律制御機構の有効性を実証するためRed Hat OpenStack Platformを導入して、システム管理者の負担軽減とサービス品質の安定を両立するという実験シナリオを具現化し、さらなる通信量の増加が予想される将来においての迅速かつ確実なサービスの安定供給を可能とする基盤作りが実現しました。

●受賞日：2017年10月20日



サービス品質の安定化を支える網・計算資源自律制御

受賞の言葉

満足いただく品質でサービスやアプリを供するために要する通信や計算にかかるリソースの量や場所を、人や環境の変化にあわせて動的かつ伸縮自在に変更するという研究室の取組に注目いただき、たいへん嬉しく思います。研究開発にご支援を頂いた研究所の皆様やご指導を頂いた多方面の方々に感謝いたします。今後、室員とともに机上検討に留まっている新規アイデアの開発システムへの実装や、標準化への貢献などを進めてまいります。

コメント／原井 洋明（はらい ひろあき）
ネットワークシステム研究所
ネットワーク基盤研究室 室長

中央が原井洋明

第22回

「震災対策技術展」横浜

ー自然災害対策技術展ー

http://www.shinsaiexpo.com/yokohama/

2018年
2月8日（木）・9日（金）
各日10:00〜17:00
会場：パシフィコ横浜Dホール
入場方法：当日登録制
※受付にて、アンケートに記入後、入場者証と交換。2日間有効

情報通信研究機構が研究開発を進める小型光ハブなどの災害対応に役立つ技術や、ゲリラ豪雨などの早期予測を目指した地デジ放送波を用いた水蒸気量推定手法の開発など、最新の研究成果を紹介します。

第21回「震災対策技術展」横浜でのNICTブースの様子

同時開催

災害・危機管理ICTシンポジウム2018

ー災害時の情報流通とプライバシー保護ー

http://ictfss.nict.go.jp/yokohama2018

※上記Webサイトにて事前登録をして下さい

開催日：2018年2月9日（金）
主　催：次世代安心・安全ICTフォーラム
　　国立研究開発法人情報通信研究機構
会　場：パシフィコ横浜
　　アネックスホール
参加費：無料

災害・危機管理ICTシンポジウム2017での講演の様子

超スマート社会の実現に貢献するナノテクノロジー

nano tech 2018

国際ナノテクノロジー総合展・技術会議

http://www.nanotechexpo.jp/main/index.html

2018年
2月14日（水）〜16日（金）
各日10:00〜17:00
会場：東京ビッグサイト
　　東4・5・6ホール＆会議棟

NICT未来ICT研究所は、2018年2月14〜16日に東京ビッグサイトで開催される国際ナノテクノロジー総合展・技術会議に出展、14日には同会場会議棟において未来ICTシンポジウムを主催開催します。

展示ブースでは、未来の光通信に資する有機光電変換素子や超伝導光子検出器などのデバイス技術について、材料から作製、実証へ至る最新の技術を紹介します。さらに、バイオテクノロジー分野からの情報通信への利用に関する研究やミリ波、テラヘルツ波の未開拓周波数領域の通信技術など、最新の未来基盤技術研究開発の展示のほか、技術移転や知財活用の紹介展示も行います。

nano tech 2017での様子

同時開催

未来ICTシンポジウム2018

〜超スマート社会に向けたICTデバイス技術の新展開〜

開催日：2018年2月14日（水）13：00〜17：00
主　催：NICT未来ICT研究所
会　場：東京ビッグサイト会議棟6F（605会議室）
参加費：無料（定員100名）

「超スマート社会に向けた既存ICTデバイスの性能限界の打破や新規な機能を有する革新的ICTデバイスの創出」をテーマとして、異分野技術や異種材料の融合、新しい原理の利用といったコンセプトのもと、光通信や無線通信、センシング、光・電子制御等の分野において技術革新に取り組む最新の研究成果を紹介します。

NICT NEWS 2018 No.1 通巻 467
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：平成30（2018）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: http://www.nict.go.jp/
Twitter: @NICT_Publicity

定期購読のお申込みはWebまたはE-mailにて承っております。
ISSN 1349-3531 (Print)
ISSN 2187-4042 (Online)

〈再生紙を使用〉