NICT NEWS
国立開発研究法人
情報通信研究機構
No.4
2020
通巻482

FEATURE

待ったなし。セキュリティ人材育成

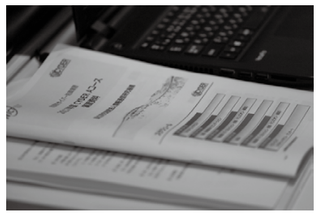
Interview

悪質化するサイバー攻撃から日本のシステムを守れ

サイバー防御演習で万全の構え

CONTENTS

NICT NEWS 2020 No.4 通巻482
国立研究開発法人情報通信研究機構



表紙写真：SecHack365のコースワークの1コマ
SecHack365は25歳以下を対象にした、1年間のセキュリティ・ハッカソンです。研究開発支援として合宿形式の集合イベントを年6回実施しています。集合イベントでは、写真のようにトレーナーからの講義・指導や、トレーニー（受講生）同士の議論などに取り組みます。

左上写真：CYDERで使われている教材
実践的サイバー防御演習CYDERでは、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ます。CYDERでは難易度と受講目的に合わせてAコース（初級）、Bコース（中級）を選ぶことが可能です。受講対象者と身に着くスキルは本紙pp.6-7をご覧ください。

Interview

悪質化するサイバー攻撃から日本のシステムを守れ

サイバー防御演習で万全の構え

ナショナルサイバートレーニングセンター

園田 道夫（そのだ みちお）〈左〉
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。SecHack365では、トレーナー及び学習駆動コースコンテンツゼミを担う。2004年よりセキュリティ・キャンプ講師及びプロデューサー及び実行委員、2007年より白浜サイバー犯罪シンポジウム危機管理コンテスト審査委員、2012年よりSECCON実行委員事務局長。博士（工学）。

佐藤 公信（さとう ひろのぶ）〈右〉
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
大学院博士後期課程修了後、高知工科大学地域連携機構助教、高知工業高等専門学校准教授を経て、2017年4月NICT入所。CYDER、サイバーコロッセオにて利用されるトレーニングマテリアルプロデューサー。SecHack356では、表現駆動コースコースマスター。SEC道後プログラム検討会委員、SECCON実行委員。情報処理安全確保支援士 実践講習講師、CISSP。博士（工学）。

サイバー空間では、日夜熾烈（しれつ）な戦いが繰り広げられている。コンピューターネットワークは世界中とつながっており、常にサイバー攻撃にさらされている。

防御するにはシステムを強化すると同時にセキュリティ担当者のスキルも必要だ。組織内部にセキュリティに詳しい要員が多ければ多いほど守りを強くできる。現在、情報セキュリティの分野では約20万人の人材が不足しているとされる。

NICTナショナルサイバートレーニングセンターでは、セキュリティ人材育成に向けて「サイバー防御演習」を立ち上げている。これは、いったいどういうものなのか。園田道夫センター長と佐藤公信主任研究員に話を聞いた。

――センターは2017年4月に発足していますが、3年間でどのように進化したのでしょうか？

園田　「CYDER[*1]」（サイダー）という「実践的サイバー防御演習」、東京2020オリンピック・パラリンピック競技大会対応の「サイバーコロッセオ」、それと「SecHack365」（セックハック サンロクゴ）という3つの演習プログラムがあります。

CYDERは、国の機関・地方公共団体及び重要インフラ等を担う方々を対象とする演習です。受講者数は年々増加し、昨年度は累計11,019人と国内最大級の規模に成長しました。

CYDERが防御専門で基本的な知識を持っていただくのが目的なのに対して、サイバーコロッセオは東京2020オリンピック・パラリンピック競技大会の運営者などに的を絞ったもので、攻撃側と防御側に分かれて攻防戦をやります。実際の攻撃に対処できるような高度な実践的スキルを身につけていただくことを目標としています。残念ながらオリンピックが延期になりましたので、今は状況を見極めているところです。

SecHack365は、セキュリティ分野のイノベーター育成を目的としたものです。25歳以下の若い人達を対象に、セキュリティ分野で独創的な技術開発を行う人材を発掘し育てるためのプログラムです（図）。

――日本は、セキュリティ分野は弱いのでしょうか？

園田　官公庁や防衛関連企業・研究所などに対するサイバー攻撃が頻発しています。しかしながら、守ってくれるセキュリティソフトウェア、セキュリティアプライアンスには日本独自のものがほとんどありません。これでは安全保障上も好ましくありません。そこで、セキュリティ分野のソフトウェアを自分たちで作れるような技術者・研究者を育てる必要があるということで、このようなプログラム（SecHack365）を立ち上げました。

セキュリティ分野に限りませんが、日本はベンチャーが育ちにくい風土です。外国、特にアメリカは非常にチャレンジ

Interview

悪質化するサイバー攻撃から日本のシステムを守れ

サイバー防御演習で万全の構え

図　SecHack365北海道回 開発駆動コース受講の様子

ングで、いいアイデアが出ると割と簡単に起業でき、経営的な面でもサポートされており、社会全体で育てていこうとしています。日本ではそういうところがまだまだ不足していると思います。

思いがけない新型コロナウィルスの感染拡大防止の取組がきっかけとなって、テレワークが増えて企業も個人もこれまで以上にネットワークに頼るようになってきました。今後ますますセキュリティ技術が重要になってきます。ネットに依存する人の数が増えると攻撃も増えるので、対応できる人材の必要性も高くなります。

そういう部分で当センターのサイバー防御演習が貢献できるのではないかと思います。

■サイバー攻撃の現状

――どんな攻撃が行われているのでしょうか？

園田　主な攻撃としては、サーバーに大量の情報処理要求を送りつけて実質使用不能にするDDoS攻撃、不正アクセスによるweb改ざん、データベースからデータを抜いてしまう攻撃、偽装メールに実行ファイルを添付してマルウェアに感染させる攻撃、そのマルウェアの一種でファイルを暗号化し暗号解除にお金を要求するランサムウェアなどがあります。

海外からの攻撃は多く、なかには国家組織が絡んだと思われるものもあり、そういう攻撃者はスキルが高いため、情報収集・データの破壊といった目的が完了したら、ログを消し去っていくケースもあります。そうなると追跡が難しくなります。

しかも、これらの攻撃手法やソフトウェアの脆弱性は、世界中にものすごい勢いで共有されていきますから、防御する側も不断の勉強と情報収集が欠かせません。

佐藤　そのような状況に対抗するために、多層防御を行い、何層にも重ねて防御しています。その一つとして人（職員）に対する教育も必要なのです。

■演習の具体的内容

――演習のシナリオはどのように作成しているのですか？

佐藤　その年のトレンドになるようなものを冒頭に掲げ、それを発火点としてシナリオを始めます。例えば、標的型攻撃が多い年は、「不審なメールが増え始めている」といった状況を作り出します。リアリティー重視で、いかにもありそうな状況を設定します。

そうして徐々にストーリーを展開していき、身につけてほしいセキュリティの知識を掲げ、自ら考える動機付けとしてもらいます。

シナリオは毎年何種類も作ります。2020年度は３つのシナリオを用意する予定です。ポイントは、インシデントをどう扱っていくかというインシデントハンドリングです。

演習を開始すると、最初のイベントが起こる。例えば、外部の機関から侵入の形跡があるようだという通報を受けたとします。その通報を受けてどう動くか。侵入の具体的な状況をどうやって調べるか、被害はどの程度で、最小限に食い止めるためにはどうすればいいのか。

このように実際にありえそうなシナリオに沿って、ログを解析し、対策や手順を検討し、安全で確実な対応に改善していく方法を学びます。

園田　小説と同じように演習のシナリオにはストーリーがあります。いわゆる起承転結です。起の部分が最も変化が必要なのですが、その時々の話題に合わせて変えることができます。その後の展開も含めて、何種類ものストーリーを「部品」として用意しておくことで、それらを組み合わせて変化のあるリアルなストーリーが構築できます。

佐藤　演習用のネットワーク環境は、NICTのStarBED（北陸StarBED技術センター、石川県能美市）というテストベッド環境を使って仮想化し実践的な演習を行います。そこには当センターで開発した「CYDERANGE（サイダーレンジ）」というサイバー演習自動化システムを用意しており、受講者の進み具合に合わせながら課題を出していきます。

――演習の難易度はどれくらいなのですか？

佐藤　CYDERは初級のAコースが1つ、中級のBコースが２つの合計3コースあります。1回の受講者数は30人ほどで、全国の都道府県で年間100回ほど開催しています。

Aコースでは1回の授業に1人の講師とサポート役の4人のチューターがつきます。受講者はその人たちと一緒になって、ひとつずつ課題の解き方を学んでいきます。ネットを使った基礎的な事前学習はしていただきますが、プログラミング言語などの知識はいりません。

園田　組織内には、様々な部署の人がいます。あらゆる業務の人達のセキュリティのリテラシーを底上げすることで、サイバー攻撃の被害を少しでも減らそうというのが演習の目的です。

佐藤　技術的な知識だけでなく、ソフトスキルも身に着けていただけるように工夫しています。例えば外部のセキュリティ担当官署やセキュリティ企業などの関係先と過不足なく連絡を取り合えるためには、専門用語を使ったコミュニケーション能力も必要です。

――CYDERで何か資格が取れるのですか？

佐藤　資格は取得できませんが、情報処理推進機構（IPA[*2]）の情報処理安全確保支援士（RISS[*3]）の資格は、3年に一度の更新のための講習を受けることが義務付けられており、この更新要件の特定講習となるようにCYDERを申請する予定です。

■学ぶ目的

――サイバーセキュリティを学ぶうえで大切なことは？

佐藤　サイバーセキュリティの基本は情報科学です。まずコンピュータとネットワークの基本を知ること。また、セキュリティ技術は進歩が極めて速いので勉強が欠かせません。

進歩が速いという意味でも、どんどん若い人材を育成していくことが大切です。しかし、課題は、日本が構造的にモチベーションを高めることがやりにくい社会であることです。

アメリカでは、資格がキャリアアップにダイレクトに関係しています。例えば、コンプティア セキュリティプラス（CompTIA Security+）を持っていれば年収4万ドル、CISSP[*4]といった資格を持っていると年収10万ドルと資格にあわせて給料がぐんと跳ね上がります。

日本の場合は、なかなかそうはなりません。ですから、モチベーションが上がるように社会構造も変えていく道筋を提示していかなければいけないと考えています。

――国立の研究機関としての役割は？

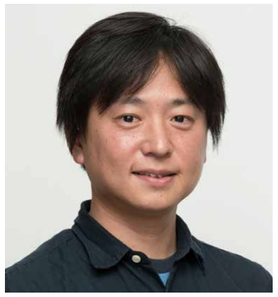
園田　民間ではできないようなことをやっていきたいです。NICTはNICTERなどのサイバーセキュリティの大規模な観測網を持っています。長年の研究で得られた技術的知見も豊富です。このような膨大なリソースを演習に活かし、日本のネットワークと社会構造を安全かつ強靭なものに変えていく一翼を担うことが我々の役割だと考えています。

*1　CYDER：Cyber Defense Exercise with Recurrence
*2　IPA：Information-technology Promotion Agency
*3　RISS：Registered Information Security Specialist
*4　CISSP：Certified Information Systems Security Professional

本インタビューは、人数、ソーシャル・ディスタンス、時間、換気、手指消毒等に配慮して行いました。

持続的な人材供給の実現を目指して

ナショナルサイバートレーニングセンターの取組



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年まで同サイバーセキュリティ研究室 研究員。2013 年より同サイバー攻撃対策総合研究センター サイバー防御研究室 主任研究員（兼務）。2016 年より同セキュリティ人材育成研究センター研究マネージャー、2017 年より現職。ネットワーク運用管理技術と、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。2007年暗号と情報セキュリティシンポジウム（SCIS）論文賞、2009年科学技術分野の文部科学大臣表彰（科学技術賞）等を受賞。博士（工学）。

電気、ガス、水道といった重要インフラ企業や政府機関までをも対象としたサイバー攻撃に関するニュースが、日常的に取り上げられるようになり、官民挙げてのセキュリティ対策が進められてきましたが、一方で慢性的なセキュリティ人材の不足も指摘されています。

ナショナルサイバートレーニングセンターでは、深刻なセキュリティ人材の不足を解消し、セキュリティ人材を持続的に供給可能な社会を実現するため、実践的サイバー防御演習「CYDER」、東京2020大会に向けたサイバー演習「サイバーコロッセオ」、そしてセキュリティイノベーター育成事業「SecHack365」の三事業を推進し、対策を進めています（図）。

■セキュリティインシデント対応要員の社会的な底上げを担う ＜CYDER＞

サイバー攻撃へ適切に対処するには、日頃からセキュリティ対策をITベンダーに任せきりにするのではなく、日常のシステム運用を考慮しながら、主体的に対処することが大切です。

ナショナルサイバートレーニングセンターでは、サイバー攻撃を受けた際に情報システム担当者が取るべき「一連の対処行動を身につけること」を目的とした、実践的サイバー防御演習CYDERを推進しています。CYDERは、国の機関、地方公共団体等の公的機関の方は無料で、またそれ以外の民間企業等の方は有料で受講することができます。CYDERでは、NICTが長年にわたるサイバーセキュリティ研究において蓄積した知見と、現実のサイバー攻撃事例を踏まえた最新の演習シナリオを用意しています。そしてNICTが有する大規模計算環境上に構築された、実際の組織のLAN環境を模した演習環境を活用して、実技（ハンズオン）を交えながら、サイバー攻撃への対応力を身に着けることができます。

CYDERは演習全体を通して得られた実践的な経験や知識を自組織に持ち帰り、それらを現場で活用することに重点を置いた内容となっています。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おり、セキュリティの初心者でも受講が可能となっています。

■東京2020大会の安定的な実現に向けて ＜サイバーコロッセオ＞

東京2020大会のような世界から注目される国際的で大規模なイベントは、攻撃者にとって格好の攻撃対象であり、より巧妙なサイバー攻撃を受けることが予想されています。

ナショナルサイバートレーニングセンターでは、東京2020大会の円滑な実施を支援するため、大会関連組織のセキュリティ関係者を対象としたサイバー演習、サイバーコロッセオ事業を推進しています。サイバーコロッセオでは、東京2020大会組織委員会とその業務受託ベンダーの職員を対象として、「コロッセオ演習」と「コロッセオカレッジ」と呼ばれる2つの形態での実践的な演習が実施されています。このうちコロッセオ演習では、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攻防戦を主体とする実機演習を通じて、CYDERよりも一段階上（図における準上級）のレベルの人材育成に取り組んでいます。「コロッセオカレッジ」は前述のコロッセオ演習を受講するうえで必要となる前提知識を補完する目的の講義演習で、ここではサイバーセキュリティに関する幅広い領域の知識を身に着けることができます。

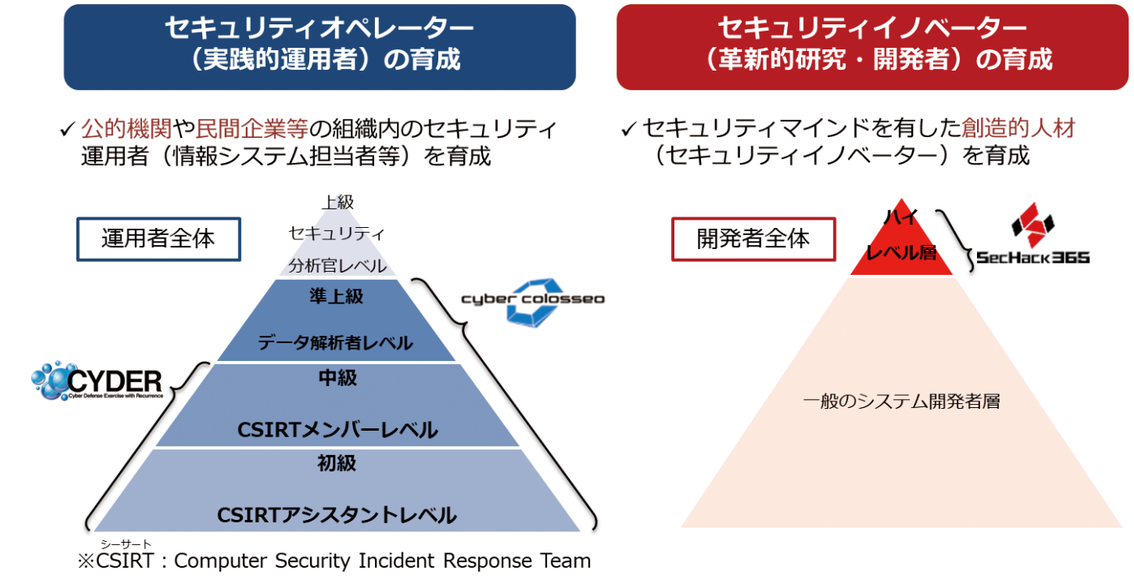


図　NICTナショナルサイバートレーニングセンターにおける三事業

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つつ、大会関係者のセキュリティ対応力の向上に、大会直前まで取り組む予定です。

■セキュリティ自給率の向上を目指して ＜SecHack365＞

世界のサイバーセキュリティ市場における日本ベンダーの存在感は、決して大きくはなく、国内でもブラックボックス化した海外製品を利用することが多いのが現状です。私たちが自らの手で自らの社会の安全を守っていくため、単に既存海外製品を「運用」するだけでなく、新たな製品等を「研究・開発」できる人材の育成を通じて、国産セキュリティ技術の開発体制を構築することにより、セキュリティ自給率を向上させることが、日本社会に求められています。

この課題に対してナショナルサイバートレーニングセンターでは、未来のサイバーセキュリティ研究者・開発者等の創出に向けて、若手のICT人材を対象に、セキュリティ技術に関する研究・開発を本格的に指導する事業SecHack365を推進しています。SecHack365は、25歳以下の学生や社会人から公募選抜する40名程度の受講者を対象に、サイバーセキュリティに関するソフトウェア開発や研究、実験、発表を一年間継続して「モノづくりをする機会」を提供する「長期ハッカソン」です。全国の一流研究者・技術者や受講者等との交流をするなかで、自ら手を動かし、セキュリティに関わるモノづくりができる人材（セキュリティイノベーター）を育てます。

本事業は2017年度に開始され、既に3期目のプログラムが完了しました。これまでの修了生らは、既に国内外のセキュリティ関連事業やイベントにおいて、目覚ましい成果を挙げつつあります。修了一年目の選抜チームが海外の著名なハッカソンイベントにおいてスポンサー賞を受賞しているほか、情報処理学会の中高生情報学研究コンテストにおいて最優秀賞を受賞した修了生や、SecHack365での成果物を活用して起業し、国内のビジネスプランコンテストで経済産業大臣賞を受賞した修了生など、活躍の事例は枚挙に暇がありません。

いずれの事業も、NICTにおいては2016年度以降に順次実施してきましたが、それでも社会的な需要を満たすには程遠い状況です。NICTのナショナルサイバートレーニングセンターでは、これまでにご紹介した三事業と並行して、より効果的かつ効率的な人材育成手法の研究開発にも取り組むことで、持続的な人材供給の実現を目指していきます。

実践的サイバー防御演習CYDER
受講のススメ

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。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、イベントや勉強会等を多数主催。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においてCYDER、SecHack365、CYDERANGE開発等の事業に携わる。SECCON実行委員長。

左から、五十里 治美、内田 陽子

五十里 治美
（いかり はるみ）
内田 陽子
（うちだ ようこ）
**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**

昨今、サイバー攻撃による被害が様々な組織で生じています。サイバー攻撃は受けた直後から適切に対処しなければ被害が急速に拡大してしまいます。サイバー攻撃による被害拡大を防ぐためには、被害を最小限に抑えるための初動対応が重要です。この初動対応を含め、インシデント発生から事後対応まで実機を使って一連の流れをトレーニングできるのがCYDERです（表1）。

■インシデント発生前に備えを

例えば災害現場において多数の負傷者が出た場合、医療関係者は患者の重症度に基づいて治療の優先順位を設定しているようです。この優先順位付けを「トリアージ」と言いますが、サイバーセキュリティにおいても同様の対応が必要で、インシデント発生後に行う「インシデントハンドリング」では、被害状況と重要度に基づいて対処の優先順位付けが必要です。

トリアージの重要性を理解したうえで、インシデント発生時には何を確認してどのように判断すればいいでしょうか。インシデントの発生後には様々なイベントが並行に立ち上がり、短期間で判断を下し、アクションを起こさなければなりません。情報システムではどのような事象として確認できるのか、組織として関係者との調整はどのようにするかなど、インシデントが発生する前に備えておくべきことがあります。

CYDERではサイバー攻撃を擬似的に発生させ、攻撃を受けた情報システム環境を提供することで、実機を使った実践的なトレーニングを行えます。インシデントハンドリングを体験することで「どうすれば検知できるのか」「被害を最小限にするためにどんな対応をすればいいのか」という気付きを得ることができます。

表1　CYDER基本情報

目的	組織がサイバー攻撃を受けた際の被害を最小限に食い止めるため、実践的に対処法を身につけること
対象	国の機関、指定法人、独立行政法人、地方公共団体、重要社会基盤事業者、民間企業など
受講日数	事前学習1時間程度＋集合演習1日　※毎年の受講を推奨
URL	https://cyder.nict.go.jp/

表2　受講対象者と身に着くスキル

	Aコース（初級）	Bコース（中級）
受講対象者	●情報システムに携わりはじめたばかりの方 ●インシデントが発生した際の対応者 ●安全に情報システムを運用したい方 ●インシデントへの備え方を学びたい方	●情報システム管理者、運用者 ●情報システムの調達・企画・開発に携わる方 ●インシデントが発生した際の対応者及び対応の指揮・管理に携わる方
身に着くスキル	●事前の備えとして何をすれば良いかを理解できる ●ベンダーからの報告書を読み解き、適切に情報共有できる ●インシデント発生時の対応の流れを理解できる	●PC, サーバー、ネットワーク機器等のログを監査できる ●CSIRTメンバー、上司、ベンダー等と情報共有し、主体的にインシデント対応ができる ●自組織のセキュリティーポリシーを見直すことができる

■CYDERのカリキュラム

現場で働く担当者は日常業務が忙しく、研修や訓練のために十分な時間を確保することが難しい状況にあります。そのような現場の声を踏まえて、CYDERではインシデントハンドリングに必要なスキルを厳選・凝縮し、1時間程度で学べる事前オンライン学習と1日間の集合演習を提供しています（表2）。

事前オンライン学習では、集合演習受講へ向けた基礎的な内容や集合演習で使用するツールの使い方等を学べます。一般的なe-Learningと同様にインターネット経由でどこからでもアクセスできます。

集合演習では、実機を使って一連のインシデントハンドリングを体験することができます。1グループ3～4名程度でグループを組み、演習シナリオに登場する組織の一員としてセキュリティインシデントに対応していただきます（図）。

各グループには、演習シナリオに登場する組織の情報システム環境を提供します。各グループに独立した環境を提供するので、この環境内で自由にサイバー攻撃や対処方法を体験・学習することができます。普段の業務では実施をためらうようなコマンド実行、思い切った設定変更等をすることも可能です。

演習で登場するサイバー攻撃やインシデントハンドリングの流れは、現実に起きたサイバー攻撃の最新動向を徹底的に分析し、毎年最新のシナリオを準備しています（表3）。

表3　演習シナリオ例

テレワーク中のさいだ省職員Sさんが使用していたソフトウェアの脆弱性を攻撃されてマルウェアに感染。Sさんが出勤して省内システムにPCを接続したタイミングでマルウェアが感染拡大。
さいだ市職員Mさんが管理するWebアプリケーションの脆弱性を悪用した攻撃者が侵入。内部サーバーの情報を攻撃者が窃取。

■Why CYDER？

有事の対処能力は日常業務を行っているだけで身に着けることは困難です。実際にインシデントが発生した際に、迅速かつ的確な対応ができるよう平時からインシデント対応能力を十分に高めておく必要があります。受講者からは「実際にやってみたら思いどおりに動けず、訓練の重要性に気付けた」という声もありました。

サイバー攻撃に対しても、毎年行う防災訓練のように備えておくことが重要です。1回の受講で終わらせることなく繰り返し異なるシナリオを体験することで、個別要素の意味や効果、影響を見極める力を高められます。学んだ内容を持ち帰って広めることで、組織のインシデント発生時の対処能力を高めることが期待できます。

■これまでのCYDER、これからのCYDER

CYDERは2013年度に総務省の実証実験として開始し、事業主体がNICTに移管され、実施体制の強化、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回程度、3,000人以上が受講可能な規模で運営しています。演習環境はナショナルサイバートレーニングセンターが開発した演習インフラCYDERANGE（サイダーレンジ）を活用しています。

今後は、集合演習で各グループに提供している演習環境をオンラインで提供するような先進的な研究開発にも取り組んでいく予定です。

図　演習風景

CYDER事業を支える事業推進室から

五十里 治美

「情報セキュリティの知識には自信が無い」と感じている皆さん、是非CYDERを受講してください。特にAコース（初級コース）は自信が無くても大丈夫。困ったときには、経験豊富な講師・チューターが手厚くサポートしてくれます。

CYDERでは「もしもの時に何をすべきか」を実際にPCを操作しながら体験することができ、「こんなことが原因でインシデントが起きるの？」「インシデント発生後はこんなに沢山の作業が発生するの？」といった気付きも得られ、高いセキュリティ意識を持つことができるようになります。

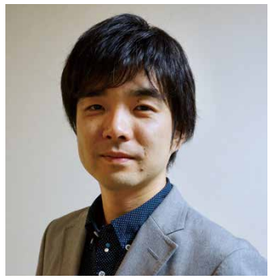
私達はCYDERが円滑に運営できるように、そしてCYDERの良さを全国の皆様へお伝えし一人でも多くの方にご受講いただけるように、縁の下の力持ちとして日々業務を遂行しています。

内田 陽子

何の知識や心構えもない状態でサイバー攻撃を受けた場合、みなさんは適切に対処できますか？CYDERは、サイバー攻撃を受けた際に適切に対応ができるように訓練するプログラムです。初心者の方からシステム運用者の方まで、講師・チューターによるサポートを受けながらインシデントハンドリングの一連の流れを体験することができます。まだ受講したことがない方はもちろんのこと、以前に受講したことがある方、皆さんのご受講をお待ちしております！

東京2020大会後も日本のサイバーセキュリティを守るために

サイバーコロッセオが残すレガシー



安田 真悟
（やすだ しんご）
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

大学院修了後、産学官連携研究員を経て、2013年NICT入所。大規模模擬環境の構築と制御などに関する研究とサイバーセキュリティ演習・人材育成への応用に従事。博士（情報科学）。

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
主任研究員

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NICT入所。主にサイバーセキュリティ演習のシナリオ開発に従事している。趣味は半田付け。

ロンドン2012大会でオリンピック・パラリンピックを対象としたサイバー攻撃が顕在化して以降、オリンピック・パラリンピックは大会の度にサイバー攻撃を受けています。サイバーコロッセオでは東京2020大会の円滑な実施を支援するとともに、東京2020大会後にも日本を支えるセキュリティ人材をレガシーとして残せるよう様々なカリキュラムを実施しています。

■サイバーコロッセオの概要

近年のオリンピック・パラリンピックはサイバー攻撃を行う格好の標的となってしまっています。ナショナルサイバートレーニングセンターでは、東京2020大会におけるそうした脅威に備え、円滑な大会運営を支援するため、セキュリティ人材育成事業「サイバーコロッセオ」を実施しています（図1）。

サイバーコロッセオは、東京オリンピック・パラリンピック競技大会組織委員会（以下、組織委員会）及び業務受託ベンダー担当者を受講対象として、組織委員会を通じて受講者の募集を行っています。2017年度に開始された本事業は、段階的に規模を拡大し、2020年には後述するコロッセオ演習3レベル（初級・中級・準上級）で220人規模の人材育成を目標としています。東京2020大会を支える組織には組織委員会関連組織のほかに外部組織もありますが、そちらについては同じくナショナルサイバートレーニングセンターで実施している地方公共団体等向け実践的サイバー防御演習「CYDER」で対象としているので、サイバーコロッセオでは組織委員会関係職員の育成に対象を絞って注力しています。

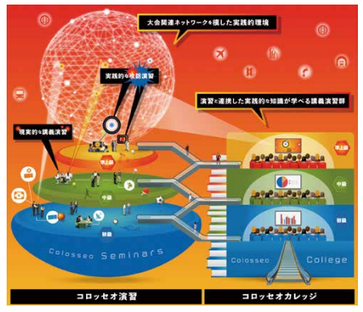


図1　サイバーコロッセオ事業

■サイバーコロッセオのカリキュラム体系

世界有数のビックイベントであるオリンピック・パラリンピックには金銭や示威的な目的で様々なサイバー攻撃が予想されます。そのような状況で大会システムを運用するためには個々人が持つ「守る技術」だけではなく、部署間の連携、信頼と協働による組織力「衛（まも）る技術」が必要です。そこでサイバーコロッセオでは、組織委員会と密に連携をとりつつ「コロッセオ演習」「コロッセオカレッジ」の2種類のカリキュラムを通じて、リアルな体験や技術的な底上げと、組織・部署間の連携醸成の両面でのトレーニングをしています。

■コロッセオ演習～攻撃者の意外なマインドを知り“衛る”を磨く～

「コロッセオ演習」は、表1に示すように初級、中級、準上級の3つレベルと、職務領域を考慮して各レベルで複数のコースを編成、合計7コースを開講しています。特に中級以上ではインシデントレスポンスのトレーニングのみならず、攻撃者の視点の演習によるトレーニングも実施しています（図2）。

表1　コロッセオ演習シナリオの種類

コロッセオ演習の種類		
レベル	種別	備考
初級 CSIRTアシスタント レベル（1日間）	初級A	購買等個人情報を取り扱わない業務に従事する受講者向けシナリオ
	初級B	個人情報を取り扱う業務に従事する受講者向けシナリオ
中級 CSIRTメンバー レベル（1日間）	中級A	代表的なWEBサービスへの攻撃を模擬サイトを用いて試行。試行結果のログの確認や影響調査を行う演習
	中級B	実例に基づく組織ネットワークシステムへの攻撃を、発覚端所から順に追跡、攻撃の全容を解明する演習
準上級 データ解析者 レベル(2日間)	準上級A	グループに分かれ、互いの組織ネットワークへの侵入をCTF形式で学び、攻撃ログの解析から対策を検討する攻撃主体の攻防戦
	準上級B	準上級AのCTF形式を継承し、攻撃バリエーションを増したペネトレーションテスト演習
	準上級C	攻撃を運営スタッフ（Red Team）が担い、受講者が自組織ネットワークを防御する防御主体の攻防戦

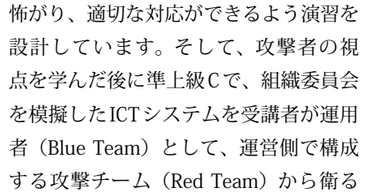


図2　コロッセオ演習準上級演習風景

一般的なサイバーセキュリティの演習は、防御手法やインシデントレスポンス等の実務的なトレーニングに重点を置きます。しかし、攻撃者の手口やメンタリティを理解せずに対応に就く場合、必要以上に攻撃者に畏怖してしまいます。

ドラマや映画のサイバー攻撃者は、一瞬でシステム内部深くまで侵入するように描かれます。しかし、実際にはかなり地道で忍耐力が必要な作業を伴います。そこで、中級では攻撃体験を含む演習、準上級A/B演習では受講者同士がチームに分かれ、互いの模擬環境に侵入する等の攻防戦形式の演習も取り入れています。普段はログやアラートとして認識する攻撃がどのような時間スケールで進行するのか、攻撃者からは対象のシステムがどのように見えるのか、攻撃の難しさや攻撃者のメンタリティも学び、正しく怖がり、適切な対応ができるよう演習を設計しています。そして、攻撃者の視点を学んだ後に準上級Cで、組織委員会を模擬したICTシステムを受講者が運用者（Blue Team）として、運営側で構成する攻撃チーム（Red Team）から衛るRed Team / Blue Team演習を行います。この演習はインシデントのトリアージ、技術的対応、対応の記録、部署間の連携など様々な現場の対応を経験し、実際の現場で柔軟に動けるように実践的な総仕上げをする演習となっています。

■コロッセオカレッジ ～個のレベルを上げ組織力を醸成する～

「コロッセオカレッジ」は、コロッセオ演習をするうえで必要な前提・周辺知識を習得し、コロッセオ演習の効果を最大化することを目的として2018年度に新設された補助講義演習群です。組織委員会は時限的な組織のため、様々なバックグラウンドの職員が大会に向けて続々と集まっている状況です。当初演習のみの事業を実施したところ、受講者のスキルのバラツキが大きく、人間関係の薄さなどでも併せて演習のレベルを保つことが困難でした。そこで、基礎知識や技術、ツール操作に関する知識を領域ごとに分け、受講者のスキルレベルを上昇させるとともに、ハンズオンやグループワークを通した横の連携を実現する20科目（表2）を設定しました。

「コロッセオカレッジ」は選択受講制で、受講者が自身の業務内容、スキルアッププラン、興味などに応じて講義を選択します。

サイバーコロッセオは東京2020大会が開催される直前までカリキュラムの実施を予定しており、「コロッセオ演習」「コロッセオカレッジ」の最終的な受講者は数百人になります。組織委員会内の様々な部署から集まった受講者が講義・ハンズオン・グループワーク・演習を通じて経験を共有する。それによる技術だけにとらわれない組織力「衛る技術」の醸成を通してサイバーコロッセオは東京2020大会の円滑な実施を支援します。

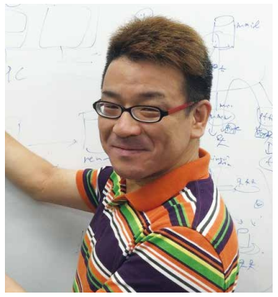
■オリンピック後にポジティブに残るレガシーに

東京2020大会では、大会をきっかけにした成果を未来につなげる「アクション＆レガシープラン」を策定しています。サイバーコロッセオの受講者のほとんどは普段は日本でビジネスを行っている企業から集まった方々です。基本的なサイバーセキュリティに関する知識や、実践的な防御・解析スキルを学んだ受講者は、東京2020大会後にも国内の様々な業種・企業でそのスキルを発揮し、大会後の日本のサイバーセキュリティを支えてくれるはずです。また、サイバーコロッセオで作成した「演習シナリオ」も、当センターの「レガシー」として、CYDERへの展開等、大会後の日本のサイバーセキュリティ人材育成に活用していきます。

表2　コロッセオカレッジ開講科目

連携コロッセオ演習	コロッセオカレッジ科目名
初級A/B	セキュリティ基礎
初級A/B、中級	セキュリティツールE
初級A/B	インシデントレスポンス概論
初級B	個人情報保護関係法令
初級B	GDPR
中級、全コース	最新セキュリティトレンド
中級、初級A/B	システムアーキテクチャ
中級、準上級	実践インシデントレスポンス
中級、準上級	セキュリティツールM
中級、準上級	脆弱性診断実務
中級、準上級	ペネトレーションテスト実務
中級、全コース	セキュア開発
準上級、中級	セキュリティツールP
準上級、中級	ログ解析実務
準上級、中級	マイクロハードニング
準上級、中級	サイバーインテリジェンス
準上級、中級	フォレンジック実務
準上級、中級	マルウェア解析実務
準上級、中級	トラフィック解析実務
準上級、中級	IRノンテクニカルスキル演習

SecHack365とは



横山 輝明
（よこやま てるあき）
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
若手セキュリティイノベーター人材を育成するSecHack365を担当。実践的なICT教育やICTによる産業貢献や社会実装の実現に関心を持つ。神戸情報大学院大学 情報技術研究科 特任准教授。博士（工学）。

塩山 英里香
（しおやま えりか）
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
SecHack365の事務局・運営を担当。

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若手人材育成プログラムです。ほかにはない365日の長期ハッカソンによるモノづくりの機会を提供することで、革新的な研究・開発ができる、「セキュリティイノベーター」の育成を目指しています。

通常のハッカソンと異なり、SecHack365では受講生（以下トレーニー）自身がセキュリティ分野で関心のある技術や問題をテーマに定め、1年間かけたモノづくりに励みます。計6回の合宿では、セキュリティやソフトウェア開発など、各分野で活躍する専門家の指導をじかに受けることができます。長期間をかけて取り組み、作っているものを他人に見せて、意見をもらいながらより良くする方法を身につけ、活動を進めます。オンラインとオフラインでの、「作る→見せる→意見をもらう→作る→…」を繰り返して専門家やトレーニーたちと切磋琢磨し、一人では開発し得なかった作品を作り上げていくことが、SecHack365プログラムの大きな特徴です。

プログラム実装や研究成果のような技術的な開発から、セキュリティ啓発のコンテンツ制作まで、セキュリティに関連する多様な作品づくりと、それらの成果を産み出せる人材の育成に取り組んでいます。

図1は、2019年度に実施したSecHack365のスケジュールです。年6回の合宿形式の集合イベントとオンライン活動によって作品づくりに取り組み、「作る→見せる」を繰り返すことで、発展的に開発する方法や、セキュリティの観点を反映した作品作りの方法を身に着けます。

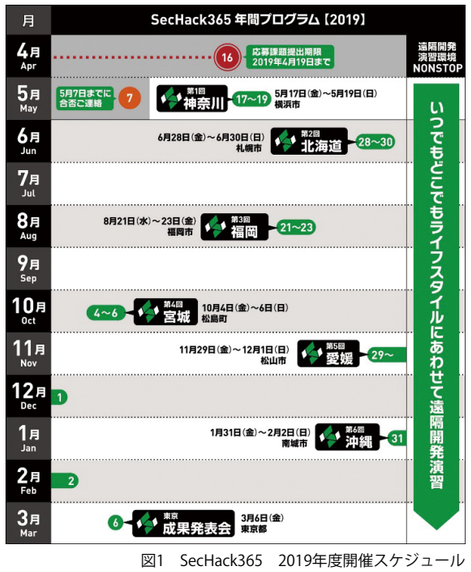


図1　SecHack365　2019年度開催スケジュール

■どんな作品づくりが行われたか

SecHack365ではトレーニーたちに、自分たちが考えるセキュリティ上の問題への解決方法を形作ることを求めます。SecHack365プログラムでは、大学や企業など、様々な分野での研究開発のスペシャリストたちを指導者役のトレーナーとして招いています。トレーニーたちは、技術的観点からの指導のみならず、継続力や発想力といった観点でのアドバイスや指導を受けながら、1年間の作品づくりを続けます。また、トレーニー間でも作品を見せ合うことで、他人に伝えること、もらった助言を作品づくりに反映する方法を体験します。このような作品づくりの場がSecHack365です。

表は、これまでの成果例の一部です。トレーニーたちは、セキュリティに関係する様々なテーマでの作品づくりに取り組んでいます。応募前から決めていたテーマもあれば、参加後に変わっていったテーマもあります。いずれの作品も、トレーニーたちが考えるセキュリティの課題に対して、自分たちで出した答えになります。

表　これまでの作品例

自動車セキュリティについて興味を持ったトレーニーたちがチームを作り、実車を利用してCAN[*1]情報の収集分析と応用について開発
不用意な個人情報の漏洩を防ぐために、tweetの文章や画像を分析して保護するtwitterクライアントの開発
セキュリティ啓発を目的とした、セキュリティをモチーフにしたゲームの開発
Python言語を用いて情報セキュリティを学ぶための書籍の執筆
QEMU[*2]を用いた、CPU上でのセキュリティ機構の実装と試験

このようにして、自分たちが問題と思うことに解決方法や作品を形づくることができるようになるのが、SecHack365の育成目標です。公式Webページには、その他の作品についても掲載していますので、関心をお持ちの方はそちらもどうぞご覧ください。

■手を動かし作ること、あきらめずに考える大切さ

トレーニーたちは応募前から決めていたテーマに取り組むこともあれば、参加後の発表や議論の中でテーマを変えることもあります。SecHack365では、何かを作り上げるための、作品が産まれる前の発想の段階から、作品をより良く磨くプロセスを経験してもらいます。このプロセスの中、短い間隔で発表機会を用意しています。作って見せる過程にて、トレーナーや他の参加者から助言をもらいながら、作品やアイデアの強みや弱みを自覚して、より良いものを目指して作り続けることに取り組みます（図2）。

多くの場合、狙いどおりのものが一回で出来上がることはありません。作り始めてみないとわからないこと、作って動かしてから気づくことも多いです。あらかじめ全てを予測しないと作り出せないということでは、新しいことを産み出すことの負担は大きくなってしまいます。また、セキュリティ的な問題についても、あらかじめ完璧なものを作ることは難しく、問題が起きた後での対処が重要です。SecHack365で身に着ける、小さく作り、見せて、作り続けていく、こうしたプロセスによって、価値を大きくする方向に最大化していき、問題があれば対処できるような、創造的なエンジニアや研究者やクリエイターになることを期待しています。

■人に見せることで得られる気づき

皆さん発表は好きでしょうか。SecHack365の中では、作ることと同じくらい、見せることを重視しています。他人に見せることに身構えてしまい、難しく考える人も多いかもしれません。けれども、他人に見せることは、様々な意見をもらえ、作るものを客観視する機会になります。見せる方法を知ると、モノづくりが孤独な作業でなくなります。こうしたフィードバックの受け取り方は、セキュリティ的な問題に対して、素早く手直しをしていく姿勢にもつながると考えています。

図2　SecHack365の実施風景

このような作って見せる場であり、継続的にモノづくりをできる人材育成を目指しているのが、SecHack365です。

＊1 CAN（Controller Area Network）：自動車の車内などで使用されるネットワーク規格のこと
＊2 QEMU（キューエミュ）：オープンソースのプロセッサエミュレータ。コンピューター内で仮想コンピュータを動作させるソフトウェアのこと

SecHack365担当者からのメッセージ

横山 輝明

何かを作り出すことは、皆さんの最も効果的な自己紹介になります。SecHack365では、1年間のプログラムによって、価値創造やセキュリティについて自分で作り磨き上げる方法を身に着けます。皆さんが考えるものを、SecHack365の中で作り上げてみませんか！

塩山 英里香

全国各地での合宿形式の集合イベントは移動も多く、プログラムも充実しているため合宿期間中は本当に大変です。でも大変な思いを共有したからこそ参加者同士の一体感やつながりもあり、修了生になって環境が変わっても交流が続いています。年齢、出身地、学校などの枠を超え、同じ目標を持った仲間が得られる機会でもあるので、たくさんの人にチャレンジしてほしいですね。未来の「SecHack365修了生」としての活躍を期待しています。

SecHack365トレーナーからのメッセージ

～情報技術を利用する全ての方と、応募を検討している25歳以下の方々へ～

猪俣敦夫　国立大学法人大阪大学　教授

専門は暗号理論、ネットワークセキュリティ。立命館大学客員教授、公衆無線LAN認証管理機構代表理事、JPCERTコーディネーションセンター理事、奈良県警察サイバーセキュリティ対策アドバイザー、セキュリティキャンプ講師ほか

ここは学校のようないわゆる学びの場ではありません。全国を移動するキャンピングカーのようなものに乗り、その中で各々作りたいものにじっくり取り組むという一風変わったスタイルをとります。共有することはセキュリティ、それだけです。育成といえばトレーナーが指導者となり進めていくのが一般的ですが、あくまでもつまずいた時の後押しをするだけ、時にはトレーニー達と一緒に悩み込むといったことも。さらには作り出してきた成果物にトレーナーの方がうらやむこともしばしば、こんなにもワクワクできる場は滅多にありません。セキュリティでよりハッピーな世界を創り出したいという方は是非。私たちは最高の場を用意して皆様からのチャレンジをお待ちしています。

柏崎礼生　国立情報学研究所　特任准教授
国立大学法人大阪大学
サイバーメディアセンター 招聘准教授

北海道大学大学院工学研究科を二度中退した後、北海道大学、東京藝術大学、大阪大学を経て現職。高可用性ネットワーク、広域分散システム、レジリエンス、萌えに関する研究業績を有する。博士（情報科学）。

セキュリティへの興味を抱きながらも「指導してくれる先生」あるいは「共通の興味を持つ友人」が身近にいないと苦悶している十代の若者がいます。そして「同年代の凄い人とじっくり話をすることができたことが何よりもの役得」と語るSecHack365修了生がいます。けれど私の観測範囲内では、初回から凄い人というのはあまりいません。1年間という時空的広がりを持つインキュベーター（孵卵器）の中で、彼ら彼女らは互いに成長させ合うのです。このことこそが、そしてそこから生まれる多様性こそがSecHack365の価値だと私は考えます。将来の好敵手はきっとここにいます。セキュリティにうずく若人は是非SecHack365へ。

SecHack365修了生の活躍例 ※カッコ内は受講時属性

2017年度優秀修了生　北村拓也さん（大学院生）

- Challenge IoT Award 2017総務大臣賞受賞
- 学生CGコンテストアート部門ノミネート
- 第15回キャンパスベンチャーグランプリ（CVG）全国大会経済産業大臣賞、ビジネス部門大賞、JVCA賞受賞（Cyship）
- 『知識ゼロからのプログラミング学習術』書籍出版
（Amazonのカテゴリー1部門で、ベストセラー第1位）
- 広島大学学長特任補佐、特任助教
- 小中高生対象のプログラミングスクールTechChance! 共同創業者
- 「株式会社Cyship」設立・代表（https://cyship.net/）
- MAKERS UNIVERSITY第3期生

2017年度優秀修了生　川島一記さん（専門学校生）

- CISCO DIGITAL JAPAN DAYS 2019 Cyship展示
- 「株式会社Cyship」設立
- ハル研究所プログラミングコンテスト３位

2017年度優秀修了生　室田雅貴さん（大学生）

- にいがたITアワード2018最優秀賞
- えちご想発×Tech 2018奨励賞
- 新潟大学発ベンチャー「株式会社Riparia」設立
代表取締役CEO（https://riparia.jp/）
- MAKERS UNIVERSITY第4期生
- 『Wide Ecosystem Accelerator－広域連携アクセラレーター-2019』に採択

2017年度修了生　ニノ方理仁さん（小学生）

- ITスーパーエンジニア・サポートプログラム“すごうで2019”採択
- 第82回情報処理学会全国大会中高生情報学研究コンテスト
中高生研究賞優秀賞受賞

2018年度修了生　窪田靖之さん（中学生）

- World Robot Summit 2018ジュニアカテゴリ ホームロボットチャレンジ人工知能学会賞
- 第82回情報処理学会全国大会中高生情報学研究コンテスト
中高生研究賞最優秀賞受賞

2018年度修了生　三橋優希さん（中学生）

- 未踏ジュニアスーパークリエイター認定（2018年度）
- BSテレ東ドキュメンタリー番組
「14歳からのスタートアップ」出演

2018年度優秀修了生　朱義文さん（高校生）

- 第81回情報処理学会全国大会中高生研究賞優秀賞受賞
- 2019CODE BLUEメイントラック：U25「Semzhu-Project－手で作る組込み向けハイパーバイザと攻撃検知手法の新しい世界」発表

セキュリティ人材育成を支える統合システム基盤環境の企画開発・運用

石川 大樹
（いしかわ ひろき）

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

●経歴
1988年　茨城県にて誕生
2010年　国内システムインテグレータ入社
2017年　NICT入所
2020年　現職

●受賞歴等
平成30年度情報通信研究機構表彰
社会貢献賞（団体）
ナショナルサイバートレーニングセンター

一問一答

Q 最近はまっていること
A 料理にはまっています。ふるさと納税返礼品の調理器具がとても優秀です。

Q 休日の過ごし方は？
A カメラを持って散歩、ツーリング、旅行、機械いじりなどです。

Q 研究者志望の学生さんにひとこと
A 多種多様な考え方、知識を持った方々と一緒に仕事をするのはとても楽しいですよ。ぜひ！

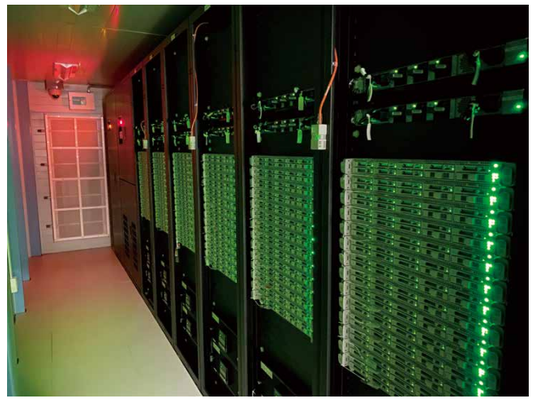
ナショナルサイバートレーニングセンターでは、実践的サイバー防御演習「CYDER」、東京2020大会に向けたオリパラ関係者向けサイバー演習「サイバーコロッセオ」、セキュリティイノベーター育成「SecHack365」の3事業を実施しています。

研究室の中にある私たち基盤チームでは、これらの3事業を支える統合インフラ基盤の企画開発・運用を行っており、現在は北陸StarBED技術センターに有する複数のコンテナ型データセンタや都内データセンタなど6つのロケーションにて30種類500台以上の機器から構成するシステムを運用しています。

統合システムを企画するにあたり、これからどうあるべきかを設計から運用まで考慮し全体を俯瞰して構想を練り上げています。開発・調達では時勢に応じて最新の技術を取り入れつつ既存設備との融和性を考慮した設計や調達物品最適化のため機能・品質・コストバランスの比較検討をしています。運用では内製化に取り組み、新機能の追加や各種リソースの効率的な配分、標準化・自動化により迅速な保守運用を実現しています。これらの取組を継続することで、品質の高い統合システム基盤を提供しています。

運用で得た知見はSecHack365においても活用し、ネットワーク運用やトラヒックの可視化、トラブルシューティングを参加者に見せていくといった取組をしていますが、深く興味を持ってくれるトレーニーもおり今後がとても楽しみです。

基盤チームの業務はひとりで行えるものではなく、チームメンバーとの連携・チームワークにより成り立っています。今後もチームの和と力を発揮し、事業を支えていきます。



北陸StarBED技術センターにて運用中のCy02コンテナ型データセンタ内部写真
メインの人材育成基盤として活用、最新の高性能サーバを大容量高速ネットワークにて相互接続。JGNやインターネット回線を通して日本全国の演習会場から演習設備を利用可能。コンテナ型データセンタの電力設備や空調設備も北陸StarBED技術センターの基盤チームメンバーを中心とした自前運用。

2020年「時の記念日」100周年!

6月10日の「時の記念日」は、671年のこの日に天智天皇が漏刻（水時計）を使って日本で初めて報時を行った故事に由来し、1920年に開催された「時」展覧会において制定されました。一方、現在の日本の標準時は、NICT（本部：東京都小金井市）において原子時計に基づいて生成され、日本全国に配信されています。

日本の標準時はどこでつくられているでしょう？

■日本標準時の生成・供給業務について

時刻、つまり「時につける目盛り・指標」については1958年から世界中の原子時計の平均によって目盛りをつけることが試行されました（国際原子時）。そして、1967年には1秒の長さはセシウム133に共鳴する電磁波が9,192,631,770回振動する時間として定義され、原子時計こそが正確な時刻や時間を表現できると認識されました。実際セシウム原子時計は大変精度が高く、数十万年に1秒ずれるかどうかというほどです。

NICT本部には、セシウム原子時計18台と、水素メーザという周波数標準器が5台程度あり、これら多くの原子時計を平均化することで時刻のふらつきを小さくしています。セシウム原子時計と水素メーザは計測システムによって相互の時刻差が毎秒計測されており、その時刻差データを基に、原子時計の時刻を1時間に1回の頻度で平均・合成、8時間ごとに周波数制御、することによって時刻が決められています。そしてさらに衛星を介して世界の原子時計と比較し、協定世界時に合うように微調整しながら日本標準時を生成しています。NICTの原子時計データは、協定世界時の基となる国際度量衡局（BIPM）の合成原子時においても高い寄与率で使われています。

生成した日本標準時の供給方法としては、まず電波時計に向けた標準電波の発射があります。これは、大鷹鳥谷山（おおたかどや）（福島県）と羽金山（はがね）（佐賀県–福岡県）の標準電波送信所から長波帯の電波（40kHz、60kHz）に乗せて送信しています。このほか、アナログ及び光の電話回線を使ったテレホンJJY・光テレホンJJY、インターネットを通してPC等の時刻合わせができるNTPサービス、タイムスタンプ等の事業者が自社の時計の時刻精度を確認するためのデータ供給、原子時計の周波数較正なども行っています。

2018年には、本部災害時のバックアップを主な目的として神戸に副局を開局しました。神戸副局にはセシウム原子時計6台と水素メーザ2台、またNTPと光テレホンJJYの設備があります。

おおたかどや山標準電波送信所

原子時計

はがね山標準電波送信所

国立科学博物館

時の記念日100周年企画展
「時」展覧会2020
期間：6月5日（金）～7月12日（日）

開館情報等については下記URLでご確認ください。
https://www.kahaku.go.jp/

「時の記念日」100周年を迎える本年、「時」展覧会を開催した国立科学博物館（当時：東京教育博物館）では、昔の「時」を学び、現在の「時」を理解し、未来の「時」に想いをはせていただけるような展覧会を開催しています。NICTからは、原子時計の原理や日本標準時のつくり方、次世代原子時計などの展示を行っています。

NICT NEWS 2020 No.4 通巻482
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2年（2020年）7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)