National Cyber Training Center

ナショナルサイバートレーニングセンターにおける セキュリティ人材育成の取組について

※本資料に記載されている事業計画等は 2022年 8月時点のものであり、今後の社会情勢等に応じて、予告なく延期・変更・中止となる場合があります。

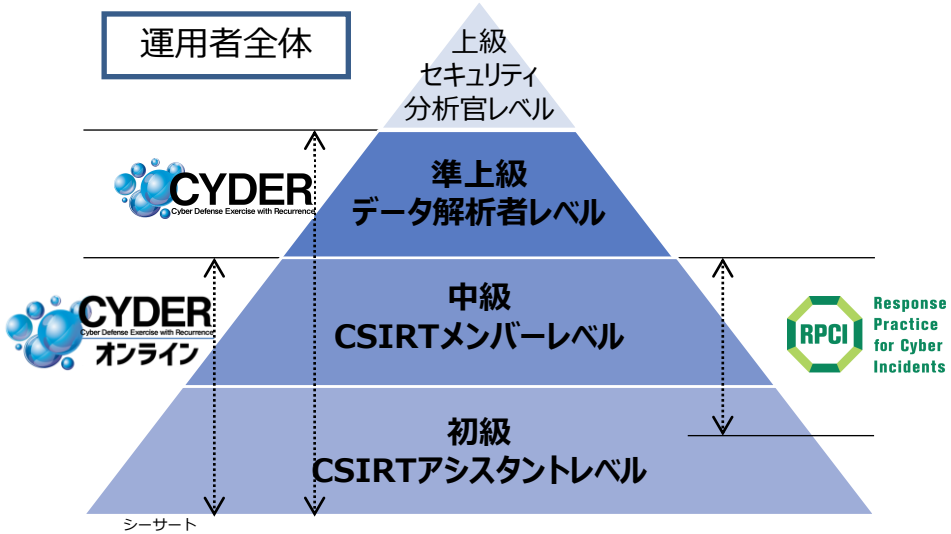
国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

「ナショナルサイバートレーニングセンター」の概要

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、「ナショナルサイバートレーニングセンター」を設置（2017年4月1日）

セキュリティオペレーター（実践的運用者）の育成

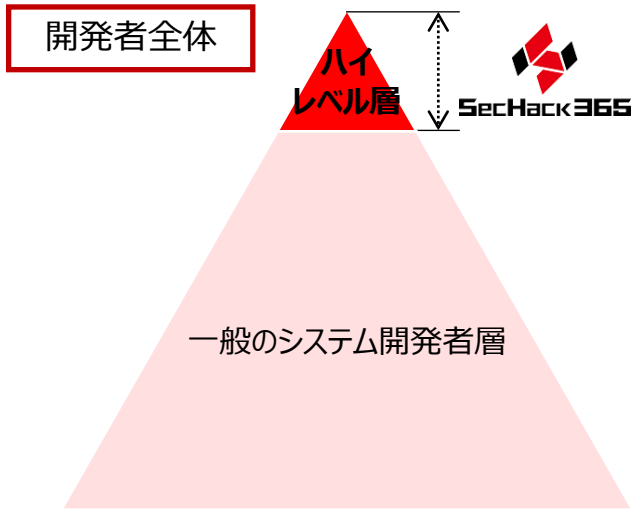
- **行政機関や民間企業等の組織内のセキュリティ運用者（情報システム担当者等）を対象**
- **所属組織が深刻なサイバー攻撃を受けた段階等（＝「有事」）における実践的なインシデント対応能力を育成**



※CSIRT：Computer Security Incident Response Team

セキュリティイノベーター（革新的研究・開発者）の育成

- **単なる「ユーザー」として既存ツールを利用するだけではなく、セキュリティマインドを持ち、革新的なセキュリティソフトウェア等を自ら「研究・開発」していくことができるハイレベルな人材を育成**



CYDER

RPCI

SecHack365

セキュリティオペレーター（実践的運用者）の育成

CYDER 実践的サイバー防御演習「CYDER」

RPCI Response Practice for Cyber Incidents

公的機関唯一の情報処理安全確保支援士向け
特定講習 実践サイバー演習「RPCI」

セキュリティオペレーター育成に関する課題

CYDER

RPCI

SecHack365

現状

- 各組織内においてインシデントが発生した際、情報システム担当者等が「直ちに」「的確な」対応を行わないと、被害を更に拡大させるおそれ
- セキュリティ人材が社会全体として不足する傾向にある

必要性

- 「平時」から、情報システム担当者等のインシデント対応能力 (外部のセキュリティ事業者や各所関係者との調整スキルや連絡体制の確立、継続的なコミュニケーション等による関係性の維持等) を十分に高めておくことが必要
- 日本全体として、早急に、多くのセキュリティオペレーターを実践対応レベルまで引き上げることが必要

課題

- **「有事」の対処能力は、日常業務を行っているだけでは、なかなか身につかない**
- **機微情報等を扱っている各組織の現用システムで、訓練のためにインシデントを発生させるのは、通常では困難**
- **日常業務が忙しくて、訓練に長時間を割くことが難しい**

求められるトレーニング像

- 平時において擬似的に「有事」の環境を構築し、その擬似環境下で、実際の機器やソフトウェアの操作を伴う実践的なトレーニングを繰り返し実施
- 現場で働く情報システム担当者等が受講可能な、コンパクトで効率的なカリキュラム

NICTによるセキュリティオペレーターの育成

CYDER
RPCI
SecHack365

NICTの「強み」

長年のサイバーセキュリティ研究による技術的知見

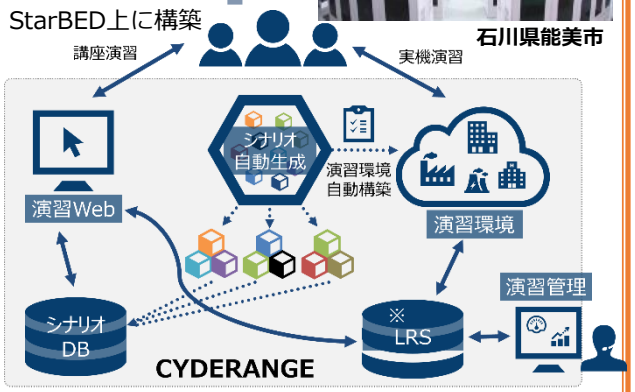
- NICTの長年にわたるサイバーセキュリティ研究で得られた技術的知見を活用し、 我が国固有のサイバー攻撃事例を徹底分析した最新の実機演習シナリオを作成
- インシデントハンドリングに最低限必要なスキルを厳選して凝縮し、コンパクトで効率的なカリキュラムを構成

大規模高性能サーバー群 NICT北陸StarBED技術センター

- **大規模性**
  大規模な組織のネットワーク環境を再現した仮想環境を構築するための大規模なサーバー群
- **運営ノウハウの蓄積**
  大規模仮想環境の効率的かつ安定的な運営に関する高度な知見・ノウハウが蓄積
- **セキュアな環境**
  インターネット等から隔離された強固な閉鎖環境

サイバー演習自動化システム CYDERANGE (サイダーレンジ)

- CYDERANGEはサイバー演習の運営に係るコストの削減と受講者のプロファイルに合わせた効果的な演習プログラムの提供を目指すサイバー演習自動化システムを2018年度から導入



※ Learning Record Store (履歴データベース)

活用

CYDER
Cyber Defense Exercise with Recurrence

サイバー攻撃への対処方法を体得

仮想空間で再現された大規模ネットワーク環境

RPCI
Response Practice for Cyber Incidents

公的機関初の情報処理安全確保支援士向け特定講習

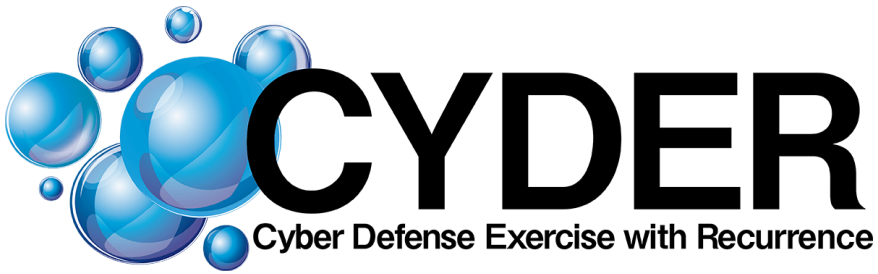
実機演習のノウハウを活かした技術に寄った講習

CYDER

RPCI

SecHack365

実践的サイバー防御演習
「CYDER」



実践的サイバー防御演習「CYDER（サイダー）」の概要

(CYDER : CYber Defense Exercise with Recurrence)

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

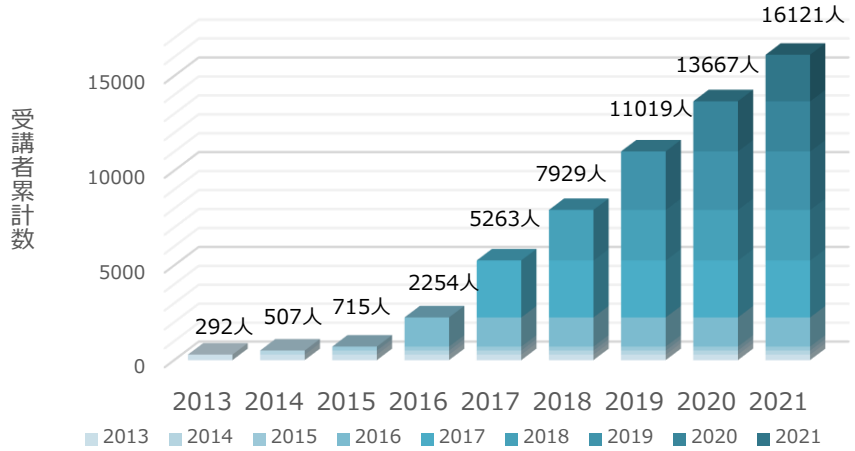
2022年度コース概要

- 毎年 **約 3,000人が受講**
- 演習は1日間 (Cコースは2日間)
- 集合 (実地) 演習のほか、オンライン演習 (個人学習)を実施
- 組織当たり1名でも複数名でも参加可能
- 重要社会基盤事業者、民間企業等は、受講料が必要

  A/B/オンラインコース … 77,000円 (税込)

  Cコース … 121,000円 (税込)

CYDER受講者数の推移 (累積数)



※グラフは集合演習の受講者数を計上。2021年度はこの他オンライン演習を641名が受講。

2022年度実施内容および対象組織

コース名	演習方法	レベル	受講想定者（習得内容）	受講想定組織	開催地	開催回数	実施時期
A	集合演習	初級	システムに携わり始めたばかりの方 (事案発生時の対応の流れ)	全組織共通	47都道府県	64回	7月～翌年2月
B-1		中級	システム管理者・運用者 (主体的な事案対応・ｾｷｭﾘﾃｨ管理)	地方公共団体	全国11地域	20回	10月～翌年1月
B-2				地方公共団体以外	東京・大阪・名古屋・つくば	13回	翌年1月～2月
C		準上級	セキュリティ専門担当者 (高度なセキュリティ技術)	全組織共通	東京	3回	10月～翌年2月
標準	ｵﾝﾗｲﾝ演習	初級	システムに携わり始めたばかりの方	全組織共通	(受講者職場等)	随時	5/24～7/19
入門		入門	インシデント発生時の対応の学習をこれから始める、または、始めたばかりの方				翌年1月～2月

※CYDERは、(ISC)² が提供する資格の認定継続に必要なCPEクレジット (継続教育単位) 付与対象の演習

CYDERのトレーニング内容（集合演習）

- 新型コロナウイルス感染症対策をしっかり取りつつ、全国47都道府県で演習を開催（年間100回程度）
- 実際のネットワーク環境を再現したリアルな環境で、インシデントハンドリングの一連の流れを、ロールプレイ形式で体験可能
- 現実に起きたサイバー攻撃事例の最新動向を徹底的に分析し、コース別に最新のシナリオを準備
- 経験豊富な講師・チューターの親身なサポートを受けながら、受講が可能
- Aコース(初級)、Bコース(中級)、Cコース(準上級)といった多彩なコース設定で、初学者から熟練者までの学びをサポート

演習シナリオ例

Aコース (2021年度)
① 複数の職員が標的型メール（Emotet）を開き感染し、横展開する
② 展開先の端末がWeb管理者のものであり、Web管理者の端末からWebが改ざんされる

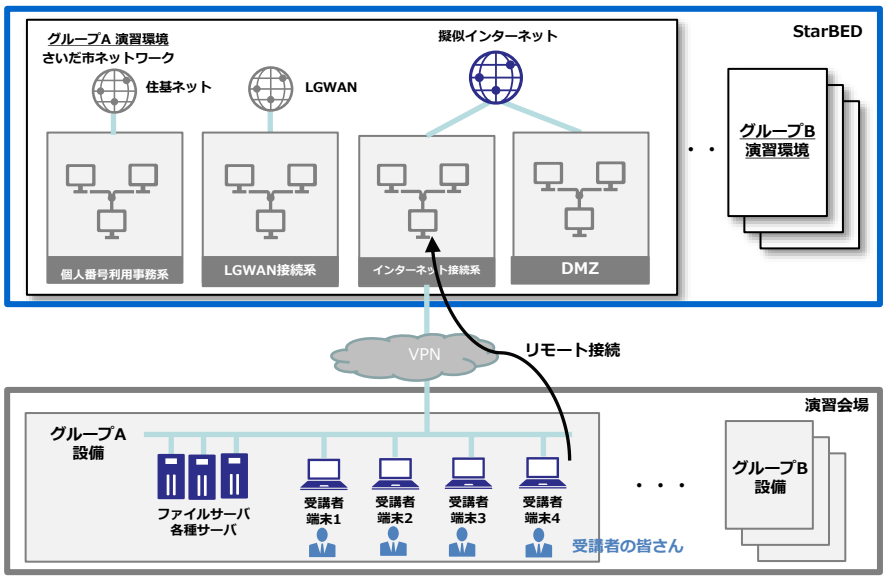
B-1コース (2021年度)
① リモートワーク端末を踏み台として、LGWANへ侵入
② そこから横展開し、展開先で情報を窃取される

B-2コース (2021年度)
① 国会議員を務める議員のメールアカウントが乗っ取られ、議員がよく連絡を取り合っていたさいだ省職員あてにマルウェア付きメールを送信する
② メールを受信した職員が点府ファイルを開きマルウェアに感染。そこを踏み台とし、省内システムがランサムウェアに感染する

Cコース (2021年度新設)
① 外部公開サーバ経由での侵害を発端とする1つの大規模インシデントを、２日間を通して解き明かす

演習舞台設定例 (B-1コース)

各グループそれぞれに提供するネットワーク構成



集合演習の流れ（Aコース、Bコース）

インシデント発生から解決、事後対応までを体験

		Aコース	Bコース
Flow 1	― 検知・連絡受付 パソコンやサーバーなどの不審な動作を検知。組織内外からの通報を受け付けます。	説明 実習 解説	実習
Flow 2	― トリアージ（優先順位付け） セキュリティインシデントが疑われる事象に対して、情報収集やログ調査などを行い、事実関係を確認します。インシデントと判断した場合には、被害状況を把握した上で重要度によって対応に優先順位を付けていきます。	説明 実習 解説	実習
Flow 3	― インシデントレスポンス（対応） 組織として、どのように対応すべきか、外部に協力を求める必要があるかなどを検討します。「証拠保全」「封じ込め」「根絶」「復旧措置（暫定対応）」を行います。	説明 実習 解説	実習
Flow 4	― 報告・公表 被害の度合いや影響を及ぼしている範囲に応じて、報告・公表します。組織内部への報告に加えて、被害者、監督官庁や警察機関などの外部関係者にも併せて報告します。	説明 実習 解説	実習
Flow 5	― 事後対応 インシデントに関わったすべての関係者が参加して「振り返り」を実施します。同様のインシデントを防ぐための今後の対応などを含め、最終報告書に取りまとめます。	説明 実習 解説	実習
			全体解説

CYDER
RPCI
SecHack365

集合演習の流れ（Cコース）

- 2020年度まで実施した「サイバーコロッセオ」のレガシー(遺産)のうち中級A, Bを、CYDERのCコース(準上級)として、合計3回開催予定(2022年度は、10月、12月、2月に合計3回)
- コロッセオでは1日間で提供していたコースを2日間に延長し、演習スケジュールに余裕を持たせることで、受講者がしっかりと技術を習熟できるように工夫

コースの具体的内容

パケット解析を主とした攻撃と対処
(2021, 2022年度)

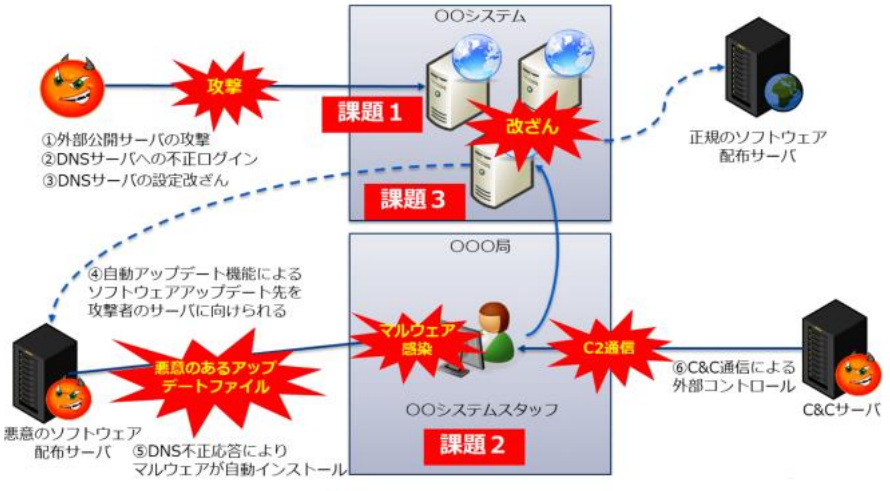
外部公開サーバ経由での侵害を発端とする1つの大規模なインシデントを解き明かす。
- 外部公開サーバへの侵害(サーバログ調査)
- クライアント端末のマルウェア感染
  - ✓Proxyログ解析
  - ✓ネットワークパケット解析
- 被疑サーバの調査

Web系を主とした攻撃と対処 (2021年度)

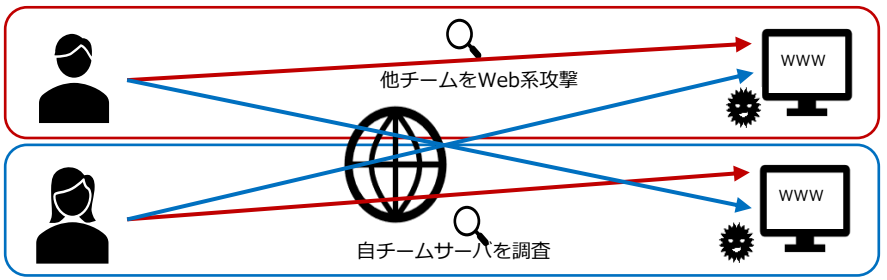
脆弱性のあるWebサイトへの攻撃や攻撃ツールを利用した攻撃体験と攻撃解析を通じて防御方法の検討を行う。
- Web系への攻撃を学ぶ
- 自チームから他チームを攻撃
- 各種攻撃ログの調査や分析を行う
  - ✓他チームの受講者が行った攻撃を解析
  - ✓受講者の攻撃以前に用意しておいた攻撃痕跡を解析

コース内容のイメージ

パケット解析を主とした攻撃と対処



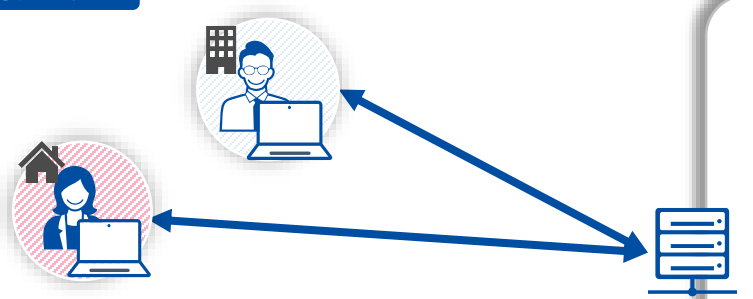
Web系を主とした攻撃と対処



CYDER オンライン演習

- 職場や自宅のパソコンのWebブラウザから演習環境に接続し、オンライン演習を受講
- 地理的・時間的要因等によりCYDER集合演習が受講できない方への対応として、CYDERオンラインコースを新設（正式版を2021年11月から実施）
- クローズドβテストを受けて改修を行い、オープンβと正式版は個人課題のみで構成

受講イメージ



スライド資料を用いた学習

クイズフォーマットの課題

録画解説ビデオで演習をサポート

仮想演習端末にアクセスして
集合演習同様に実機演習も実施

ID登録・受講フロー

ステップ1	新規アカウント作成（ID登録）
ステップ2	コース申込
ステップ3	演習日の予約
ステップ4	事前学習受講
ステップ5	オンライン演習受講

CYDERオンライン演習 令和4年度の実施計画

4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
	5/24		7/19								
	標準コース								入門コース		

CYDER

RPCI

SecHack365

公的機関初の情報処理安全確保支援士向け特定講習
実践サイバー演習「RPCI」

RPCI

Response
Practice
for Cyber
Incidents

公的機関初の情報処理安全確保支援士向け特定講習
実践サイバー演習「RPCI（リプシィ）（Response Practice for Cyber Incidents）」の概要

NICTが持つ大規模演習環境を活用してリアリティを高めたインシデントハンドリング演習。
公的機関初の**情報処理安全確保支援士向け特定講習**[*1]として、提供開始。

[*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。（詳細：https://www.meti.go.jp/policy/it_policy/jinzai/tokutei.html）

講習名称	実践サイバー演習「RPCI（リプシィ）」 ～大規模演習環境を活用してリアリティを高めたインシデントハンドリング演習～			
対象者	**情報処理安全確保支援士**、その他サイバー防御演習に関心のある方など			
講習形態	事前オンライン学習と集合演習（**ハンズオン＆グループワーク形式**）			
受講日数	1日間	**定員（1回あたり）**	32名[*2]	
受講料	88,000 (円/税込)	**受講時間**	8.5時間	
対象分野	**主な分野**	デジタルプロダクト運用	**関連分野**	脆弱性診断・ペネトレーションテスト
令和4年度開催日程[*3]	6月16日（木）、7月2日（土）、7月14日（木）、8月18日（木）、9月15日（木）、10月20日（木）、11月17日（木）、12月3日（木）、12月16日（金）、1月19日（木）			
開催会場	NICTイノベーションセンター（千代田区大手町）			

習得できるスキル

- **Wiresharkを利用した特定のプロトコルのパケット解析**
- **Nmapを利用したネットワークアクセスコントロールの適正動作確認**
- **Hydraを利用した、自らが管理するネットワーク機器への侵入試験**
- **ネットワーク機器への侵入リスク軽減策等の説明能力**
- **CISOに対する優先度をつけた再発防止策の提案**

[*2] 緊急事態宣言中は1回あたりの定員を少なく設定し、新型コロナウイルス感染症対策を徹底して開催
[*3] 全10回　追加開催はニーズに応じて検討・調整予定

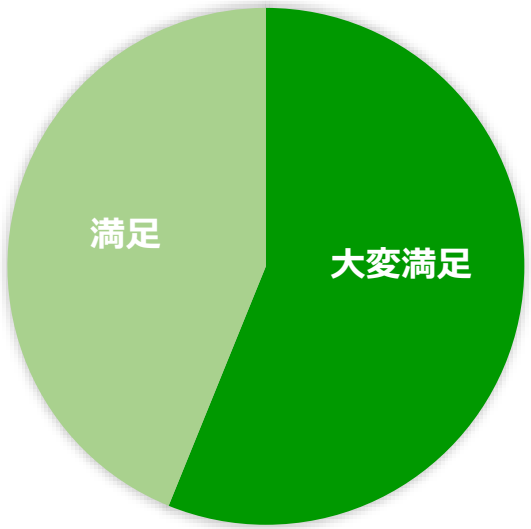
新型コロナ感染症対策

- **会場入り口での検温**
- **新型コロナの代表的症状がないことを確認、誓約書の提出**
- **CO2センサーにて換気状況を測定**
- **サーキュレーターを使用した室内の換気**

CYDER
RPCI
SecHack365

実践サイバー演習「RPCI（Response Practice for Cyber Incidents）」アンケート結果(2021年度)

講習の満足度をお聞かせください（大変満足５－４－３－２－１不満足）



満足度

100%

受講者全員が大変満足・満足と回答

- **普段の業務では行うことのできない実習（ハンズオン）**は、非常に貴重な経験となった。
- 実際にインシデントが起こった場合に行う手順・操作を把握することができた。
- 事前学習、当日の資料、解説がわかりやすかった。
- 個人的に難しいと感じる課題もあったが、**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むことができた**。
- IR対応について知識として把握している部分はあるが、**実践に近い形で経験することができ**、どのようなことについて考えておく必要があるのか（決めておく必要があるのか）などを理解することができた。

CYDER

RPCI

SecHack365

セキュリティイノベーター(革新的研究・開発者)の育成

セキュリティイノベーター育成プログラム
「SecHack365」

セキュリティイノベーター育成に関する課題

現状

- 我が国のセキュリティ・ベンダーの存在感は、世界規模で見ると決して大きいものではなく、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

必要性

- 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には、既存のセキュリティソフトウェア等を単に「ユーザー」として利用するだけではなく、新たに自ら「研究・開発」していくことができる人材の育成が必要

課題

- **マルウェア検体やその痕跡データなど関連データと、それらを安全に利用して研究・開発を行うことができる「研究・開発環境」が必要**
- **実績・経験がある一線級の「研究者・技術者」から、「技術指導・助言」を得ることが必要**

求められる人物像

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)

NICTによるセキュリティイノベーターの育成

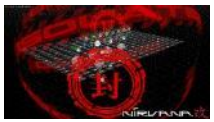
CYDER
RPCI
SecHack365

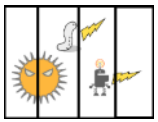
NICTの「強み」

遠隔開発環境「NONSTOP」

- NICTは、クラウド型で遠隔からも安全にマルウェア研究等を行うことができる遠隔開発環境「NONSTOP」を開発し、外部との共同研究やNICT自身の研究に利用
- NICTが大規模なサイバー攻撃観測網を用いて長年に渡り収集した現実の攻撃データ等を数十万規模でデータベース化し、研究に活用できる形式で提供

大規模高性能サーバー群

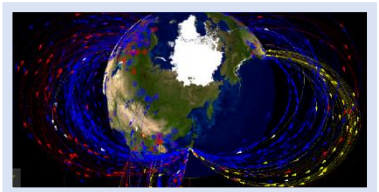


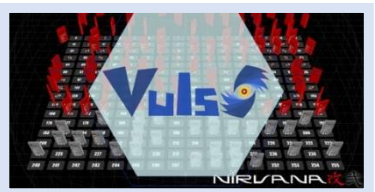


北陸StarBED技術センター
@石川県能美市

研究・開発に関する知見・人的資源

- NICTの研究者・技術者は、長年のサイバーセキュリティ研究を通じて、NICTER、NIRVANA、DAEDALUS、STARDUSTといった、最先端の研究・開発の「モノづくり」を行い、そのノウハウを蓄積





活用

SecHack365

トレーニング受講生に対して、「NONSTOP」へのアクセス権を特別に付与することで、いつでもどこからでも安全な環境下で、豊富なマルウェア検体等を使用しつつ研究・開発の実践的トレーニングを行うことが可能

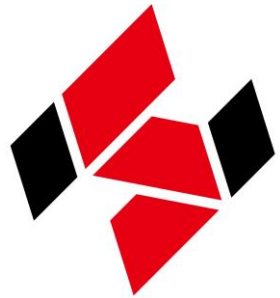
これらNICTの研究者・技術者を核として、NICTの研究分野における人的ネットワークを活用し、外部の有志の研究者・技術者の協力をも得ることにより、一線級の研究者・技術者陣による本格的な技術指導・助言を行うことができる

CYDER

RPCI

SecHack365

セキュリティイノベーター育成事業
「SecHack365」



SecHack365

セキュリティイノベーター育成プログラム「SecHack365（セックハックサンロクゴ）」の概要

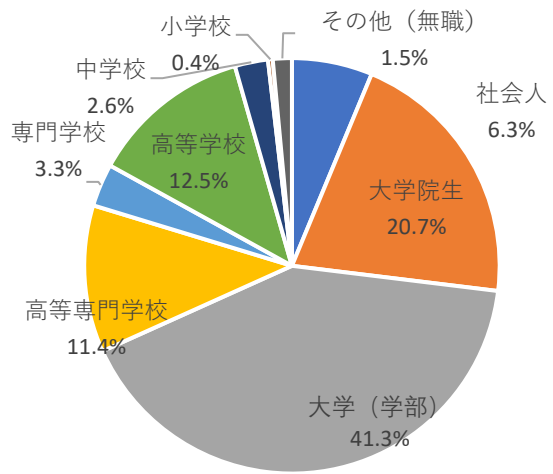
自ら手を動かし、セキュリティに関わる新たなモノづくりができる人材（セキュリティイノベーター）の育成に向けて、若年層のICT人材を対象に、NICTの持つ長年の研究開発のノウハウや、実際のサイバー攻撃関連データとそれらを安全に利用して研究開発が行える環境を活かした、1年をかけて本格的にセキュリティ関連技術の指導を行うプログラム

対象者

- **日本国内に居住する**
  25歳以下の若手ICT人材
  （学生、社会人、無職等※）

※2021年度より25歳以下の無職・無収入者へも補助

受講生属性（2017～2022年度）



年間プログラム例(2022年度)

特長

年6回の集合イベント

アイデアソン・ハッカソンのイベントを年6回実施し、継続的に開発指導します。

学生向け支援

学生は受講費用等※を全額補助。学業との両立についての相談や指導も実施。
※旅費等実費相当分

NICTならでは

サイバーセキュリティの研究開発のノウハウや、攻撃データ等を活用できる“NONSTOP”が利用可能。

最先端技術の体験

ゲスト講演や先端企業の見学で発想力やプレゼンテーションスキルを強化。

オンラインでの指導

オンラインで利用可能な開発環境を提供。チャットやタスク管理ツールを活用した継続的な指導。

「SecHack365」のプログラム内容例

CYDER
RPCI
SecHack365

1年間のプログラム例

4月	募集開始・審査選考 選考結果発表	
5月	第1回集合イベント ・キックオフ、交流 ・アイデアソン	アイデア出し テーマ検討
6月	第２回集合イベント ・コースワーク	
8月	第３回集合イベント ・企業見学、コースワーク ・全員のテーマ発表	テーマの決定 テーマの発表 レビュー デモ準備
9月	修了生イベント SecHack365 Returns	
10月	第４回集合イベント ・デモ展示 ・作品へのフィードバック	デモ展示 ポスター作製 プレゼン練習
12月	第５回集合イベント ・審査会へ向けた発表練習 ・表現の練習とフィードバック	
2月	第６回集合イベント ・全員発表 ・優秀修了作品審査会	デモ展示 ポスター展示 プレゼン発表 フィードバック
3月	成果発表会・修了式	ポスター展示 プレゼン発表





コース概要

- 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支援。
- モノづくりのアプローチが異なる複数のコースを提供。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。
- 各コースに修了生アシスタントを導入。コースワークでの指導補助の役割を担った。

01 表現駆動コース
アイデアを形にする過程で、その価値を最大化しサービスを磨き上げるコース

02 学習駆動コース
興味ある技術や作りたいものに対して付加的な学習をしながら開発するコース

03 開発駆動コース
まずは実装を作り上げることに重きをおく、開発指導に特化したコース

04 思索駆動コース
思索を通じて問題を深掘りしたうえで開発し、問題解決を行うコース

05 研究駆動コース
研究的プロセスに基づいたアイデア、仮説立案と検証評価を重視したコース

SecHack365実施風景（オフライン開催）

現地企業訪問・見学

講義

ポスター展示

デモ

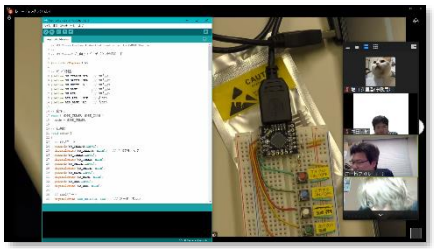
コースワーク

成果発表会

SecHack365実施風景（オンライン開催）

オンライン講義の様子

オンラインでのコースワーク・トレーナーコンテンツの提供



講演

オンライン最終成果発表

SecHack365 修了生の継続支援

➢ 修了生後の活躍機会の拡大とコミュニティの土台作り

コースごとの修了生アシスタントの導入

各コースごとに修了生アシスタントを2名配置し、コースマスターの指示のもとで通年の指導補助に従事。従来はイベント回ごとの招待制という方法だったが、通年の指導で積極的な参加を依頼。
アシスタントからの自発的な企画案もあり、アシスタント同士のつながりが修了生コミュニティの強化にもつながっている。

オンラインでの修了生アシスタント参加の様子

修了生アシスタントの指導への参加や修了生の活躍機会の拡大

アシスタントも講義を実施し、現役トレーニーへのフィードバックなどで指導へも参加。その他にも、事業説明会での発表や質疑応答などSecHack365の周知活動においても修了生の活躍の場が増えている。

➢ 修了後の成果の収集とコミュニティの継続

修了生の成果の収集として修了生ポータル開発

修了生向けの連絡、修了生からの成果情報の登録サイトとして、初期バージョンを開発。2021年度に実験運用を続けながら2022年度はさらに改善して運用予定。

9月実施予定の修了生イベント「SecHack365 Returns 2022」 参加申し込みの案内、修了生からユーザレビューを反映し、修了生との連絡ツールとしての活用のほか、成果を収集しポートフォリオ化を目指す。

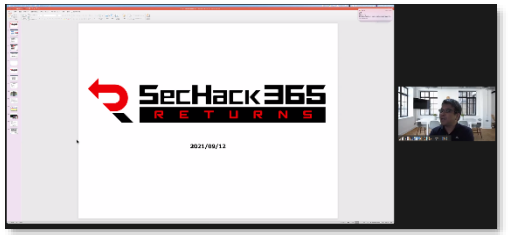
SecHack365 修了生の継続支援

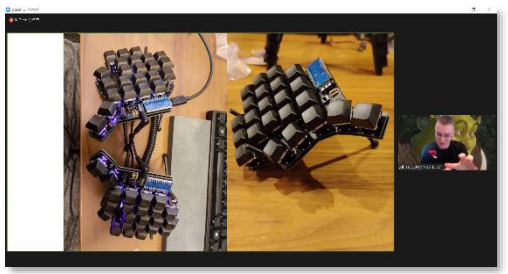
➢ 修了生イベント「SecHack365 Returns 2021」の実施

活動報告の機会および活動継続の支援、交流等を目的としたイベントであり、運営側としても毎年修了後の状況確認と成果の情報収集の機会となっている。

日　時：2021年9月11日(土)
開　催：オンライン（ZOOM使用）
時　間：13:00～18:00
参加者：約120名程度
　　修了生171名中123名から返答、83名が参加。
　　（2017年度生８名、2018年度生25名、2019年度生26名、
　　2020年度生24名）
内　容：修了生による活動報告、BoF、講演、意見交換

参加者名	修了年度	Beyond発表タイトル
宮川慎也	平成30年	継続した地域情報化の為のコミュニティ活動と運営
山本悠介	平成30年	SecHack365の成果物を使ってセキュリティ・キャンプで講師しました
古川菜摘	平成30年	SecHack365アシスタント企画の裏側(仮)
コートニー エリオット	令和元年	RNA折りたたみ博士、回路図設計自動化、自作キーボード、競技プログラミングなどの話
古田陸太	令和2年	公開鍵の公開に気をつけろ
石川琉聖	令和2年	物理鍵の仕組みと開け方
芦田裕飛	令和2年	BitcoinのP2Pを軽く解読してみた（仮）





SecHack365 修了生の継続支援

➢ 修了後の活動状況と成果

2017年度から2021年度の修了生の活動については、修了生からの報告、修了生ポータルへの登録などで情報を得たものに限られるが、こうした修了後の呼びかけに対して8割近い回答がある。

種別	件数
他事業採択	31
出版・執筆	13
研究発表・論文登録	25
学会・論文等受賞・表彰	48
新聞・テレビ・ネット掲載	28

【受賞の例】
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
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
情報処理学会 優秀論文発表賞
コンピュータセキュリティシンポジウム 最優秀論文賞
情報危機管理コンテスト 文部科学大臣賞・経済産業大臣賞
情報通信システムセキュリティ（ICSS）研究賞

【他事業採択の例】
未踏IT人材発掘・育成事業　採択
未踏IT人材発掘・育成事業　スーパークリエータ選出
異能ベーションプログラム　採択
ITスーパーエンジニアサポートプログラム“すごうで”　採択

【起業の例】
株式会社 Riparia (リペリア) 2017年度修了生
株式会社Cyship(サイシップ) 2017年度修了生
HarvestX株式会社（ハーヴェストエックス） 2017年度修了生
【大学発ベンチャー】
Defios（デフィオス）2020年度修了生

【セキュリティ専門業への進路例】
NRIセキュアテクノロジーズ株式会社
株式会社サイバーディフェンス研究所
サイバートラスト株式会社
株式会社セキュアブレイン
株式会社 Flatt Security
三井物産セキュアディレクション株式会社
株式会社ラック