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におけるセキュリティ人材育成に向けた取り組み

国立研究開発法人 情報通信研究機構
ナショナルサイバートレーニングセンター
佐藤公信

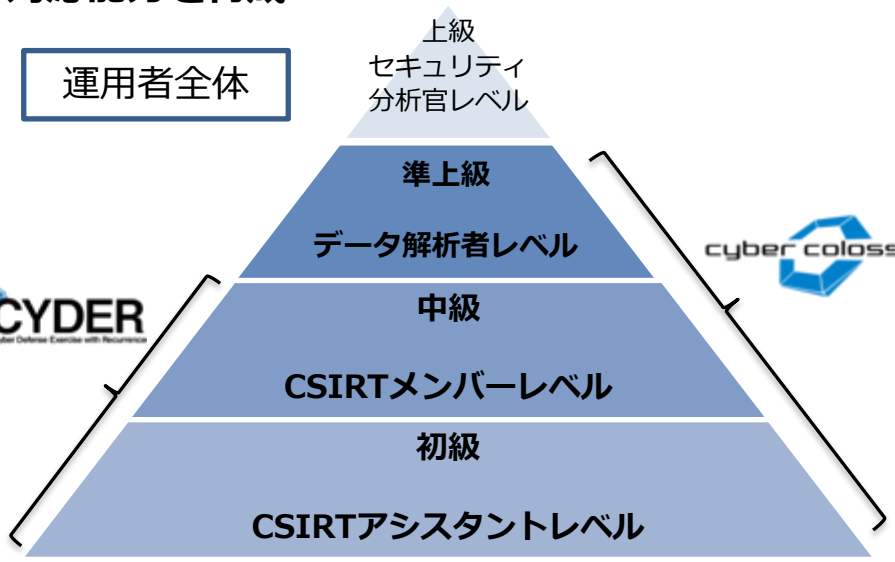
「ナショナルサイバートレーニングセンター」の概要

○ 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（2017.4.1）

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**

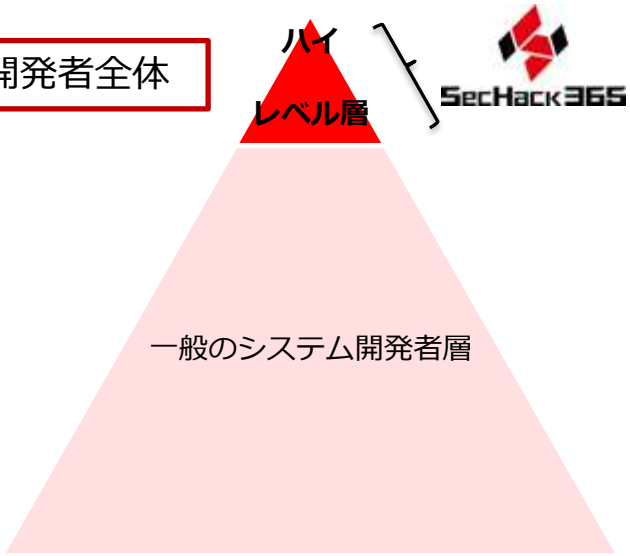
運用者全体



セキュリティイノベーター（革新的研究・開発者）の育成

- ✓ **セキュリティマインドを持ち，既存ツールの運用にとどまらず，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**

開発者全体



※CSIRT（シーサート）：Computer Security Incident Response Team

セキュリティオペレーター育成に関する課題

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

「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を十分に高めておく必要

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エ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の「強み」の活用による課題解決

大規模組織のネットワーク環境を擬似的に構築する必要性

↓

NICTが有する大規模サーバー群「StarBED（スターベッド）」の活用

注：単に大規模なサーバー群（ハード）があればよいというものではない。

1．仮想環境の構築・運営ノウハウ
　効果的なサイバートレーニングを実施するためには仮想環境を受講対象組織別にきめ細かく最適化することが望ましいが，そのためには大規模な仮想環境の再構築作業が頻繁に発生することになる。

2．セキュアな環境
　サイバーセキュリティに関する実践的なトレーニングはマルウエア検体等を実際に動かして行われるものであるため，インターネット等から隔離された強固な閉鎖環境の中で実施することが求められる。

最新のサイバー攻撃事例をベースとしたリアルな演習プログラムを，コンパクトに提供する必要性

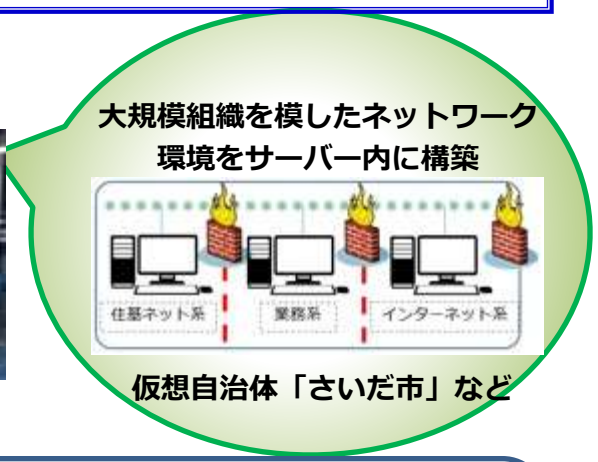
↓

NICTの長年のサイバーセキュリティ研究による技術的知見の活用

NICTによるセキュリティオペレーターの育成
～①大規模高性能サーバー群SrarBED～

NICT北陸StarBED技術センター（石川県能美市）に設置された大規模高性能サーバー群StarBEDを活用し，サイバートレーニング用に，大規模組織のネットワーク環境を忠実に再現した仮想ネットワーク環境を構築

StarBED **大規模高性能サーバー群**



○ 大規模性
大規模な組織のネットワーク環境を忠実に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の知見・ノウハウが蓄積
例) 大規模かつリアルな演習環境の効率的・迅速な環境構築技術、多数端末の同時並行運用技術、等

○ 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

※NICTは，2002年から，大規模なネットワークシミュレーション等を行う実験施設として，多数のサーバー群からなる常設のテストベッド環境「StarBED」を構築し，運用開始　その後も順次，規模等を拡大
→StarBED活用事例：P2P型ファイル共有ソフトのトラヒック検知関係実験，クラウドコンピューティング技術の試験環境実験，8K非圧縮対応の映像蓄積配信ノード性能評価実験 等多数

NICTによるセキュリティオペレーターの育成
～②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

インシデント分析センタ
（ニクター）
NICTER

対サイバー攻撃アラートシステム
（ダイダロス）
DAEDALUS

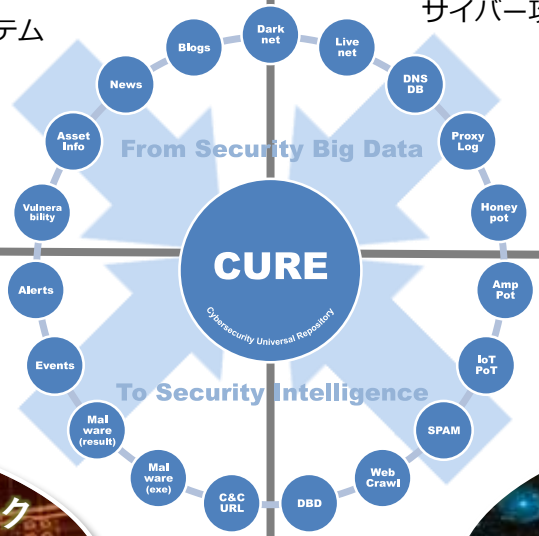
Passive

ネットワーク可視化システム
（ニルヴァーナ）
NIRVANA

サイバー攻撃統合分析プラットフォーム
（ニルヴァーナ・カイ）
NIRVANA改

Global（無差別型攻撃対策）

（標的型攻撃対策）Local



リフレクション攻撃専用ハニーポット
AmpPOT※

IoTマルウェア専用ハニーポット
IoTPOT※

サイバーセキュリティ
ユニバーサル・リポジトリ
CURE

Active

※横浜国立大学/独Saarland大との共同研究

NICTによるセキュリティオペレーターの育成（まとめ）

○ StarBED等を活用し，組織のネットワーク環境を，仮想空間で忠実に再現
○ 仮想空間において，サイバー攻撃を擬似的に発生
○ インシデントハンドリングに必要な能力を習得するための実機演習を1日に凝縮して全国展開


大規模高性能サーバー群
StarBED

北陸StarBED技術センター
@石川県能美市

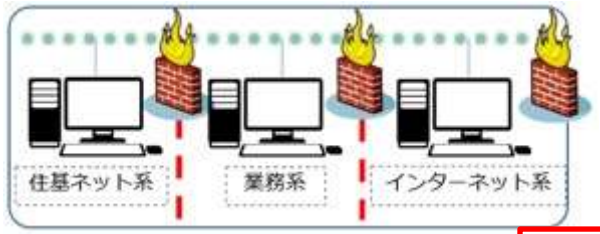
・長年にわたるサイバーセキュリティ研究で得られた技術的知見を活用
・我が国固有のサイバー攻撃事例を徹底分析した最新の演習シナリオ

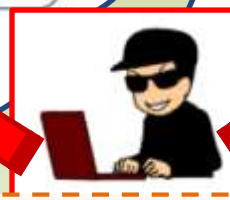
仮想空間で忠実に再現された
大規模組織のネットワーク環境

サイバー攻撃への対処方法を体得

北陸StarBED技術センターにリモート接続し，仮想組織の情報システム担当者等として，インシデント検知から対応，報告までの一連の流れを実際の機器やソフトウエアの操作を伴って体験しながら学習

仮想自治体「さいだ市」など





CYDER
Cyber Defense Exercise with Recurrence

cyber colosseo

仮想空間における擬似的サイバー攻撃

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)

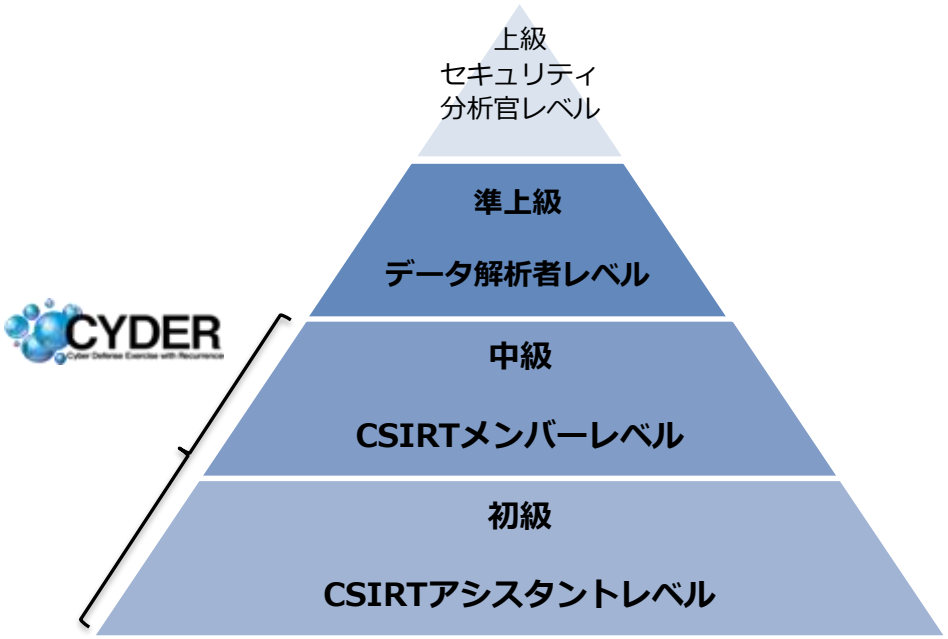
行政機関，重要インフラ等の情報システム担当者等が，組織のネットワーク環境を模擬した環境で，実践的な防御演習を行うことができるプログラムを提供することにより，数千人規模でセキュリティオペレーターを育成

コース概要

受講者の習熟度に応じて**Aコース及びBコースを開催**

・**Aコース**
CSIRTアシスタントレベル・平成29年度新設コース
全59回（平成29年度終了）

・**Bコース**
CSIRTメンバーレベル
・**B-1コース**（地方公共団体向け）
全21回（平成29年度終了）
・**B-2コース**（国の行政機関等向け）
全20回



運用者全体

CYDERの対象組織及び開催規模

2020年には，セキュリティ人材が全体として約20万人不足するとの指摘もあり，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必要。

CYDERは，サイバーセキュリティ基本法に規定される特に重要な組織を，まずは優先的に対象とし，全国47都道府県で，数千人規模でセキュリティオペレーターを育成。

対象組織

※サイバーセキュリティ基本法にて規定

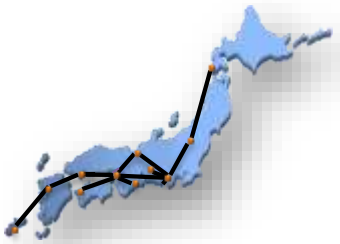
- ✓国の行政機関
- ✓地方公共団体
- ✓独立行政法人・指定法人
- ✓重要社会基盤事業者

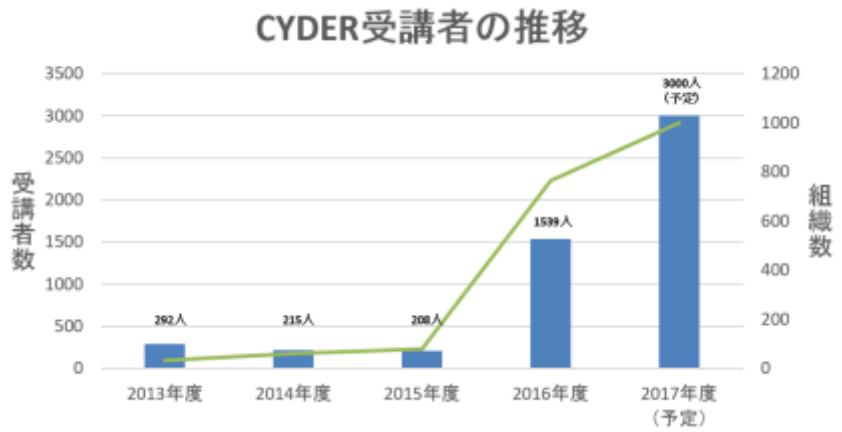
※　情報通信，金融，航空，鉄道，電力，ガス，医療，水道，物流，化学，クレジット，石油等（13分野）

開催規模

- ✓ 全国47都道府県
- ✓ 合計100回
- ✓ 3,000人以上

※2017年度実施





CYDERのトレーニング内容

○演習舞台設定
CYDERの演習舞台（仮想組織のネットワーク）は，コース別に最適化された仮想環境を構築

※ 例えば地方公共団体向けのB1コース（仮想自治体「さいだ市」）では，総務省が示す自治体情報システム強靭性向上モデルに沿った強靭性向上後の庁内システムを忠実に再現

○攻撃・対処シナリオ
CYDERの演習で使用されるサイバー攻撃や，それに対処する検知，解析，封じ込め，報告，復旧等の流れは，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，毎年最新のシナリオを準備

平成29年度演習シナリオ

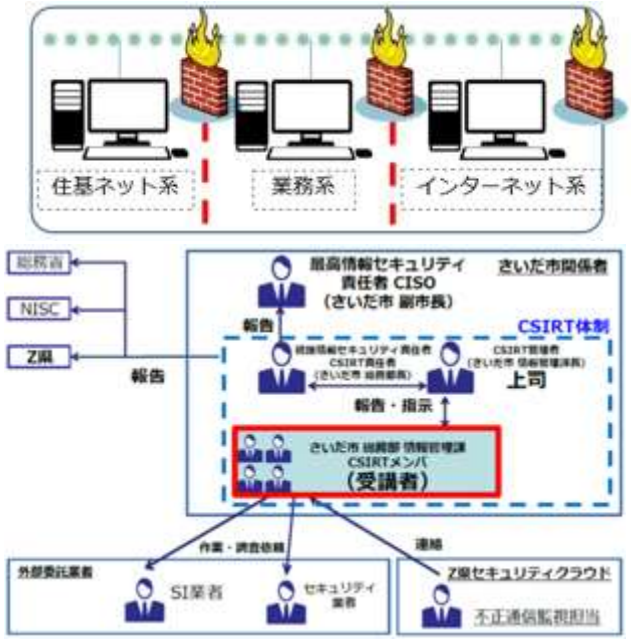
Aコース
① 職員が標的型メールを開き，ウイルスに感染
② その職員の端末から庁内の他の複数のネットワーク機器へ感染が拡大

B-1コース
① さいだ市が住民向けサービスを提供しているWebサイト（Webアプリケーションフレームワーク）の脆弱性を突かれ，管理者ページの改ざんが発生
② それを起点とし，庁内システム内にマルウェアが感染拡大

B-2コース

※ 演習シナリオは，最新のサイバー攻撃事例をふまえて，毎年度，最新のものを準備

演習舞台設定



※B-1コース

2017年度CYDER(Aコース・B-1コース）開催結果

CYDER Aコース及びB-1コースの全日程が11月までに終了。開催結果は以下の通り。

開催結果 （平成29年度）

Aコース 全59回（ 11/7終了）

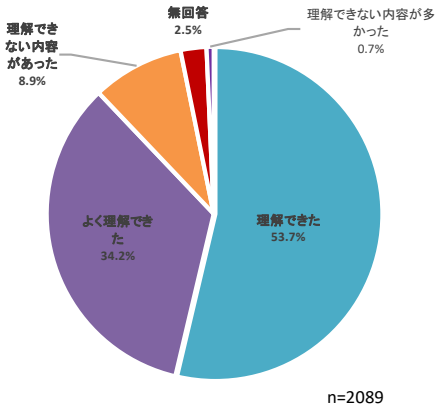
	全体数	1回あたりの平均値
申込数	1,737人	約29人
受講決定数	1,620人	約27人
受講者数	1,477人	約25人

B-1コース 全21回（11/9終了）

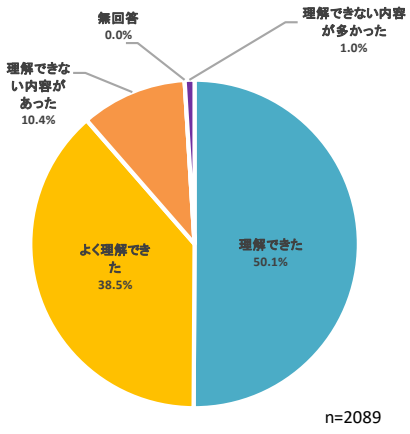
	全体数	1回あたりの平均値
申込数	736人	約35人
受講決定数	703人	約33人
受講者数	649人	約31人

集合演習＆事前オンライン学習の理解度調査（受講者アンケート） ＊Aコース+B1コース

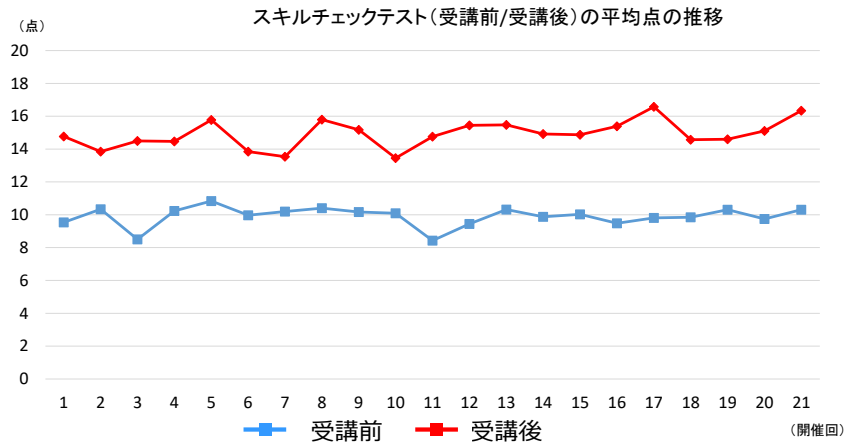
「事前オンライン学習」の内容は理解できましたか？



集合演習は，理解できましたか？



スキルチェックテスト平均点の推移 ＊B-1コース



東京2020大会開催に向けた実践的サイバー演習「サイバーコロッセオ」の概要

東京2020オリンピック・パラリンピック競技大会関連組織のセキュリティ関係者が，大会開催時を想定した模擬環境で攻撃・防御双方の実践的な演習を行うことにより，高度な攻撃に対処可能な高度な能力を有するサイバーセキュリティ人材を育成

サイバーコロッセオ実施計画の策定・公表（平成29年12月7日）

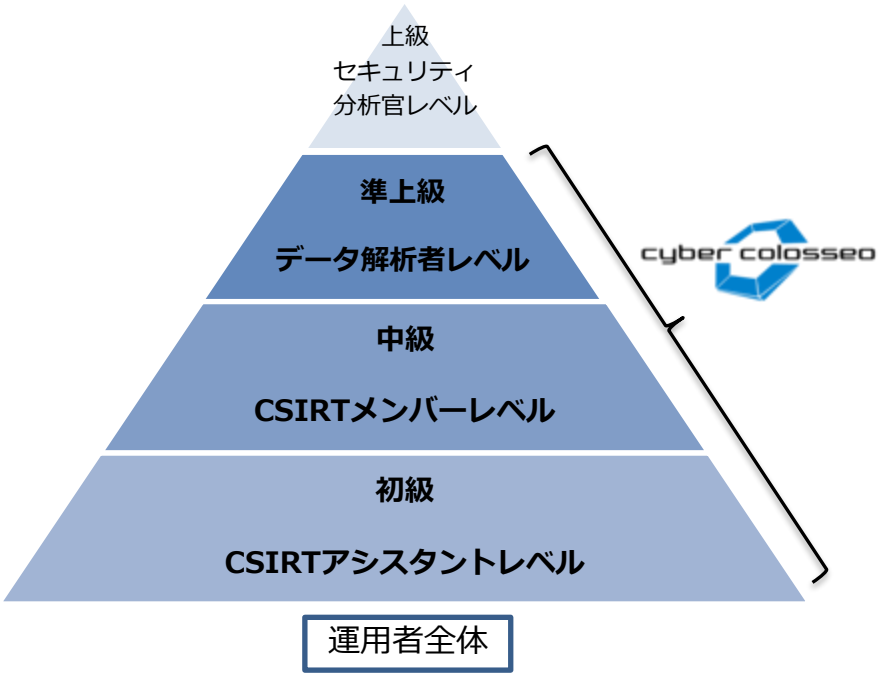
東京2020オリンピック・パラリンピック競技大会まで3年を切る中，必要な能力を兼ね備えた人材を大会開催までに段階的・計画的に育成していくことを目的として，NICTは，関係省庁・関係団体等と協議の上，平成29年12月7日「東京2020オリンピック・パラリンピック競技大会に向けたサイバーコロッセオ実施計画」を策定・公表

コース概要

受講者の習熟度や業務の性質等に応じて，
初級・中級コース及び準上級コースを開催

- 初級・中級コース
  CSIRTアシスタントレベル， CSIRTメンバーレベル
  - オンライン学習（1 時間程度）
  - 実機演習（1日）

- 準上級コース
  データ解析者レベル
  - 高度セキュリティ講義（1日）
  - 実機演習（1日）

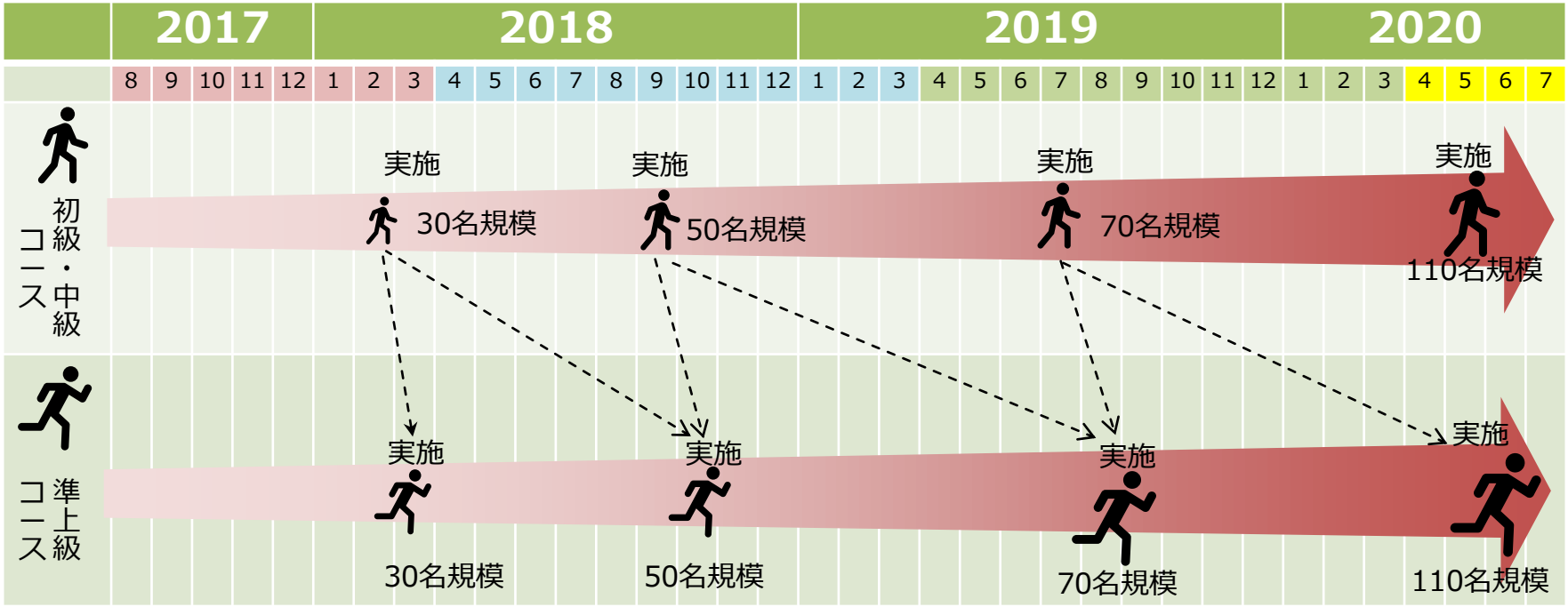


サイバーコロッセオの対象組織及び開催規模

大会開催時には高度かつ多様なサイバー攻撃を集中的に受けるおそれがあることを考慮し，サイバーコロッセオは，大会関係団体のうち最もコアな役割を担う，公益財団法人東京オリンピック・パラリンピック競技大会組織委員会を対象とする。

開催規模等

○ 東京大会開催までの3年間を通じて継続的なトレーニングを実施
○ 最終的に約220人のセキュリティ担当者等を育成予定（段階的に規模を拡大）
○ NICTイノベーションセンター（大手町）にて実施



※ 表中の目標人数は現時点において組織委が想定する数字であり，今後，組織委側のニーズを踏まえつつ，必要に応じて見直しを行う予定

サイバーコロッセオのトレーニング内容

○演習舞台設定
サイバーコロッセオの演習舞台（仮想ネットワーク）は，東京大会の公式サイト，大会運営システム等のネットワーク環境を忠実に再現して構築

○演習イメージ（準上級コース）
大会開催時に想定されるサイバー攻撃を擬似的に発生させることができるようにし，本格的な攻防戦等を繰り返し実施

攻防戦によるサイバー演習

○攻防戦
受講者が複数チームに分かれ，自組織のネットワークの守備と他チームのネットワークへの攻撃を両方体験することで，攻撃者側の視点をも踏まえたハイレベルな防御手法の検証及び訓練を行う演習

※ 攻防戦のほかに，
フォレンジックやバイナリ解析の速さ等を競うコンテスト形式の演習などを開発予定

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

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等を単に「運用」するだけにとどまらず，新たなセキュリティソフト等を自ら「研究・開発」していくことができる人材の育成が必要

課 題

革新的なセキュリティソフト等を研究・開発する実践的なトレーニングを行うためには，

- ✓ 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」を得る必要

NICTの「強み」の活用による課題解決

マルウェア検体等を安全に利用して研究・開発を行う「研究・開発環境」を構築する必要性

↓

NICTが有する遠隔開発環境「NONSTOP（ノンストップ）」の活用

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」を得る必要性

↓

NICTの研究開発に関する知見・人的資源の活用

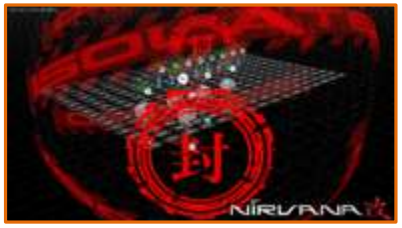
NICTによるセキュリティイノベーターの育成
～①遠隔開発環境「NONSTOP」～

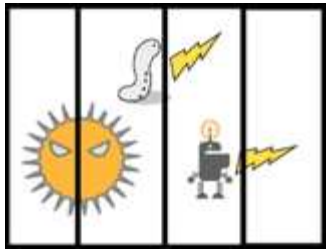
・NICTは，サイバーセキュリティ研究用に，クラウド型で遠隔からも安全にマルウエア研究等を行うことができる遠隔開発環境「NONSTOP」を開発し，NICT自身の研究に利用

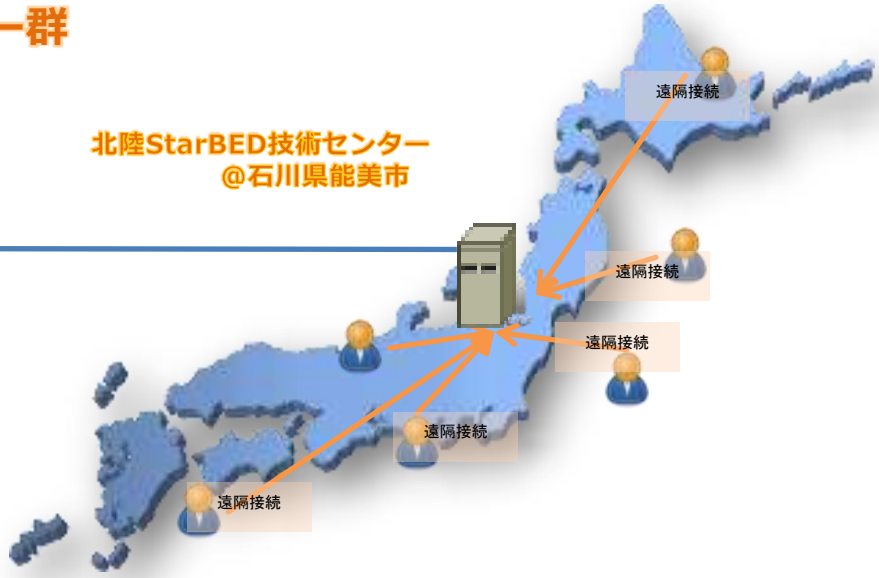
・NONSTOPには，NICTが長年続けてきた大規模なサイバー攻撃観測網により収集した現実の攻撃データ等が数十万規模でデータベース化され，研究用に活用できる形式で蓄積

・トレーニング受講生に対しても，この「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，豊富なマルウエ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

StarBED 大規模高性能サーバー群



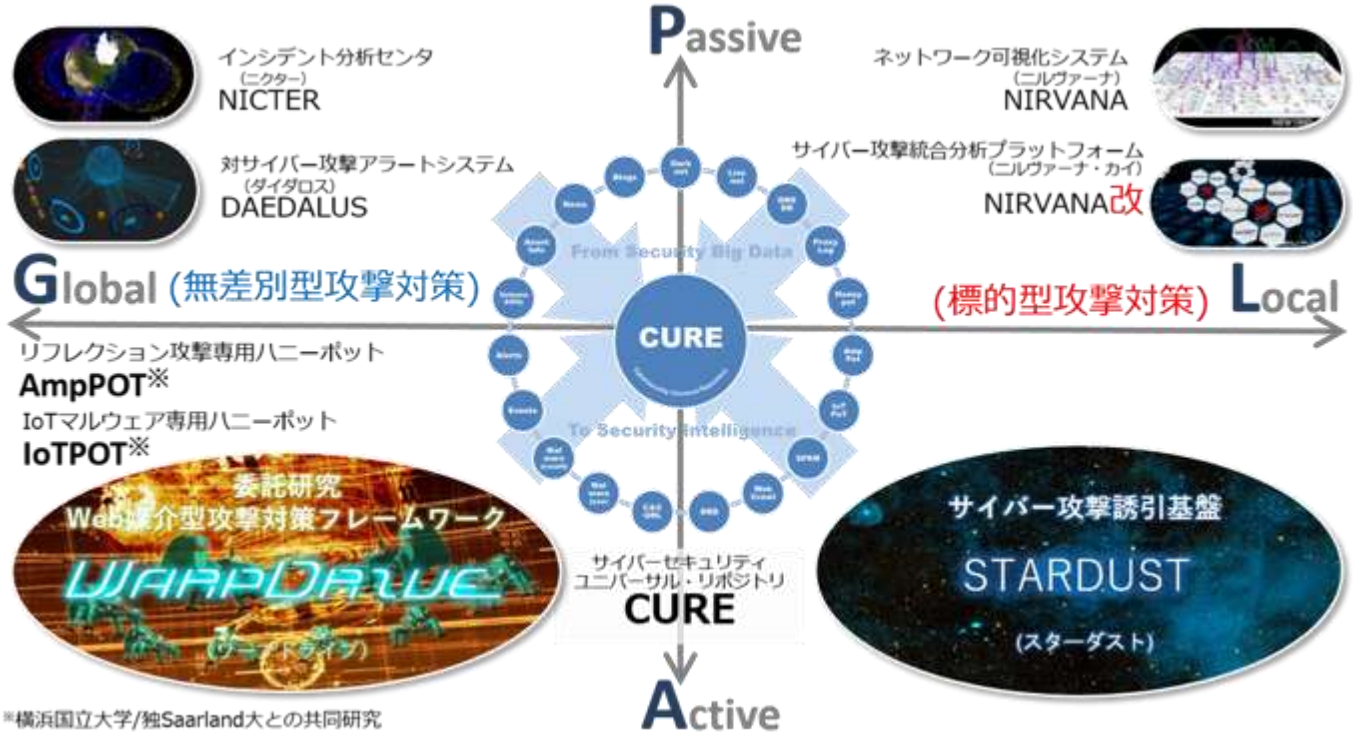




NICTによるセキュリティイノベーターの育成
～②研究・開発に関する知見・人的資源～

・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

・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。



NICTによるセキュリティイノベーターの育成（まとめ）

○NICTが有する最先端の研究開発ノウハウや，大規模なサイバー攻撃観測網により収集した現実の攻撃データ，研究者用に構築された研究開発環境等を活用
○第一線で活躍する研究者・技術者が，継続的かつ本格的に指導

大規模高性能サーバー群

StarBED

遠隔開発環境”NONSTOP”
を活用し，遠隔接続

座学講座

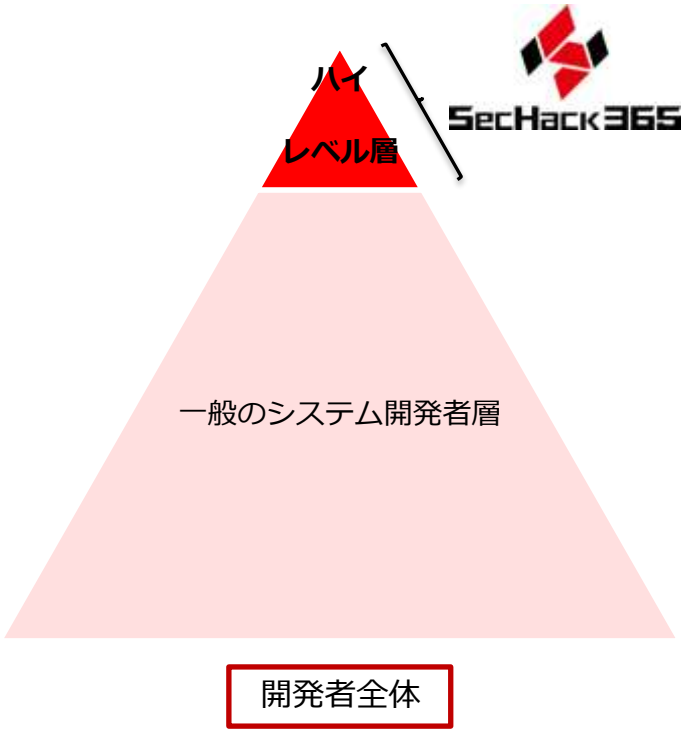
アイディアソン・ハッカソン

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

■ **未来のサイバーセキュリティ研究者・起業家の創出に向けて，NICTの持つサイバーセキュリティの研究資産を活用し，若年層のICT人材を対象に実際のサイバー攻撃関連データに基づいたセキュリティ技術の研究・開発を1年をかけて本格的に指導する新規プログラム。**

対象者

✓ **学生，若手社会人**を対象とした早期人材育成



H29年度 募集状況

募集期間	：2017年4月3日 (月) ～ 2017 年4月28日 (金)
応募資格	：日本国内に居住する25歳以下の若手ICT人材
応募数	：358名
受講決定数	：47名 （内訳　成年30名/未成年17名・男性43名/女性4名 ※2017.5.9受講者決定時点）

「SecHack365」のプログラム概要

プログラム概要

NICT の強みを活かした育成事業

- ✓ アイディアソン，ハッカソン，遠隔研究・開発，演習の組み合わせによる**総合的能力開発**
- ✓ **1 年**という長期間の取り組みにより教育効果を増大
- ✓ NICT が有する最先端の研究開発のノウハウ，研究資産 (攻撃データ等) の利活用

！ 継続的な研究開発環境の提供

- ✓ 受講者はハッカソンの実施日以外の期間も，北陸 StarBED 技術センター (石川県) に整備された遠隔開発環境 (“NONSTOP”) に自宅等から接続し，研究・開発を継続
- ✓ 北陸 StarBED 技術センターに NICT が収集したサイバー攻撃の実データを集約し研究・開発に活用

！ 反復的なイベントによる技術の深掘り

- ✓ 受講者で構成されたチームごとにサイバーセキュリティ関連システムの議論と研究・開発を行う
  (計 5回＋成果発表会1回)
- ✓ セキュリティ倫理教育，研究者による最新のセキュリティ技術の講義も実施
- ✓ 実施回ごとに開催地を変えるなど，趣向を凝らしたイベントで柔軟な発想，議論を誘起

ハッカソンのテーマ例

・攻撃検知　・自動防御　・自動解析　・脆弱性の発見　・修復　・犯罪的な徴候の発見　etc.

「SecHack365」により期待される成果等

期待される成果等

研究者の育成

- ✓ 成績優秀な学生受講者は NICT における**インターンとして研究を指導**するほか，国内研究会等における研究発表を目指す　※優秀者（若干名）に対し，海外派遣も実施予定
- ✓ 企業関係者との交流の場も設ける

研究・開発へのフィードバック

- ✓ 有望なアイディア・研究成果があれば **NICT の研究開発に応用**

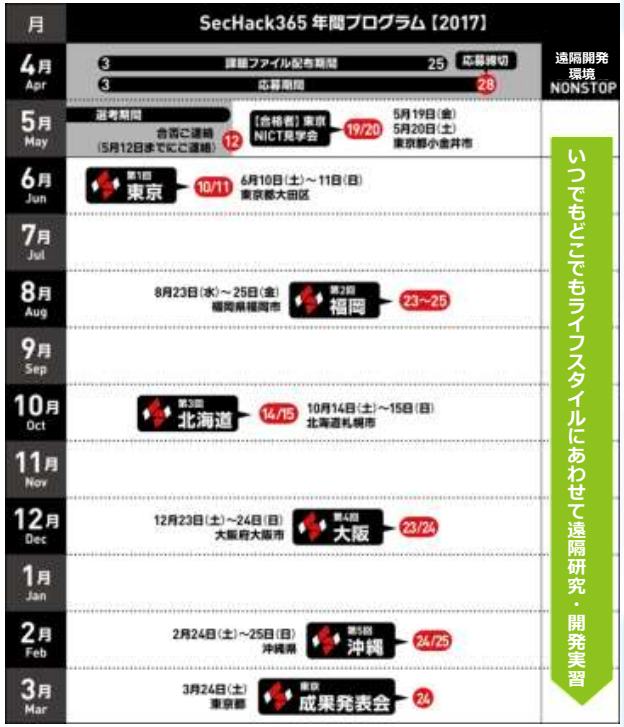
SecHack365コミュニティの形成

- ✓ SecHack365の修了生が引き続き，次年度以降の受講生の相談相手やファシリテータに

⇒　各年度の修了生が楽しく集まる，持続的で厚みのあるコミュニティの形成
⇒　1年間の受講期間で終わるのではなく，長期的な能力開発につなげることが可能に

SecHack365 実施状況

SecHack365年間プログラム

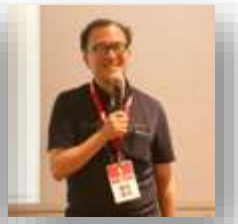


第1回東京(蒲田)回
6/10-6/11

富士通株式会社の全面的な協力を得て
FUJITSU（フジツウ） Knowledge（ナレッジ） Integration（インテグレーション） Base（ベース） PLY（プライ）
にて開催

- オリエンテーション
- アイデアソン
- グループディスカッション＆発表
- トレーナーによる講義等
- 倫理教育



第2回福岡回
8/23-8/25

- 特別講義：ＬＩＮＥ（ライン）株式会社
- 縁日（トレーナーによるハンズオン演習）
- ハッカソン　・倫理教育


第1回東京回～
第4回大阪回まで開催済

SecHack365 実施状況

第3回北海道(札幌)回
10/14-10/15

・ハッカソン
・縁日（トレーナーによるハンズオン演習）
・株式会社さくらインターネット石狩データセンター見学
・特別講義：北海道大学　町村教授（情報セキュリティと法）

第4回大阪回
12/23-12/24

・ハッカソン
・特別講義①：大阪大学　柏崎講師（研究ってなんだ（開発とのつながり））
・特別講義②：パナソニック株式会社
・発表、展示
・トレーニーとトレーナーの相談タイム

Training&Collaboration Room(TCR)のご紹介

トレーニング＆コラボレーションルーム　ティーシーアール

平成29年12月12日よりTCR本格始動　CYDER B2コース（国の行政機関等向け）開始

Training & Collaboration Room (TCR) は，CYDER・サイバーコロッセオ受講者等が能動的に参加できるトレーニングなどの場の提供と，その他外部連携コラボレーションの加速を目的として，NICTイノベーションセンター(大手町)内に設置された常設の会場です。

投影画像に
書き込める電子黒板
場所を選ばず
アイディアを書き出し
ディスカッション

大画面190インチ
スクリーン

画面のワイヤレス転送で
複数人のプレゼンターが
場所を選ばずプレゼン

可動式電子黒板3台

サイズ固定ではなく
インストラクション形態に
あわせ柔軟に拡張できるデスク

大規模高性能サーバー群

StarBED

北陸StarBED技術センター
@石川県能美市

大容量回線
（JGN）

大容量回線（JGN)に直接接続しており、
StarBEDへの高速接続が可能