

NICT における 新たなサイバーセキュリティへの取り組み

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
サイバートレーニング研究室 室長
衛藤 将史

- ナショナルサイバートレーニングセンターの事業概要と実績
 - CYDER
 - CYDER 演習デモ
 - サイバーコロッセオ
 - SecHack365
- NICT 第 5 期中長期計画における事業方針
 - CYDER、CYDER オンライン
 - SecHack365
 - 人材育成オープンプラットフォーム
- おわりに

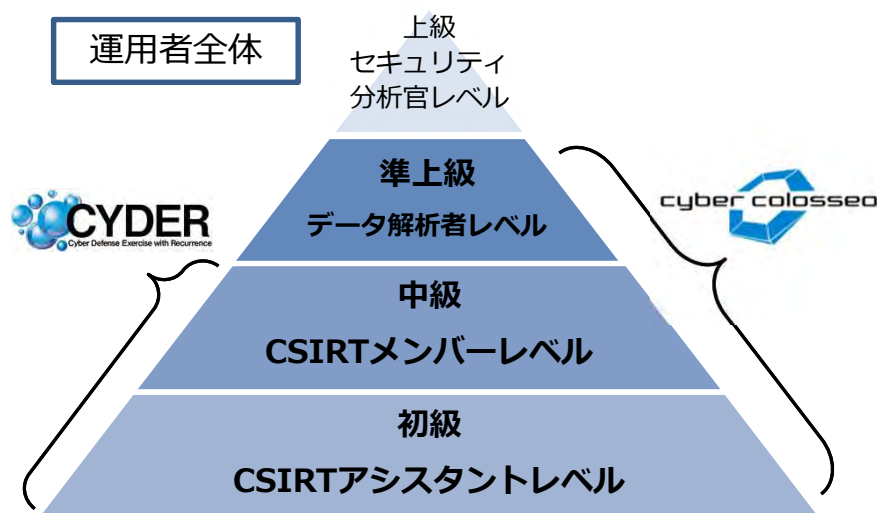
ナショナルサイバートレーニングセンターの概要



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（2017年4月1日設置）

セキュリティオペレーター （実践的運用者）の育成

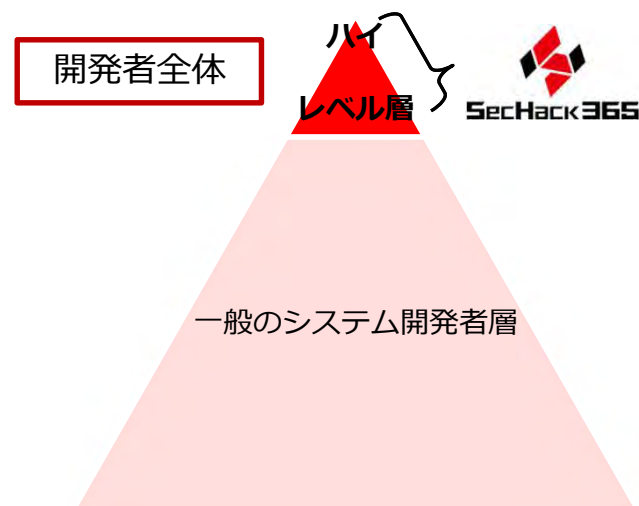
- 行政機関や民間企業等の組織内のセキュリティ運用者（情報システム担当者等）を対象
- 所属組織が深刻なサイバー攻撃を受けた段階等（＝「有事」）における実践的なインシデント対応能力を育成



※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

- セキュリティマインドを持ち、既存ツールを単に「ユーザー」として利用するだけではなく、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



ナショナルサイバートレーニングセンターの概要



セキュリティオペレーターの育成

サイダー
CYDER
Cyber Defense Exercise with Recurrence

(実践的サイバー防御演習)

仮想空間における
擬似的サイバー攻撃

擬似攻撃者

マイナンバー
利用事務系

LGWAN
接続系

インターネット
接続系

仮想自治体「さいだ市」など

仮想空間で忠実に再現され
た
大規模ネットワーク環境

NICT北陸StarBED技術センター
石川県能美市

新世代超高速通信
網

NICT 大容量回線
(JGN)

サイバー攻撃への
対処方法を体得

対象とする組織

- ＞ 国の機関等
- ＞ 地方公共団体
- ＞ 重要社会基盤事業者
- ＞ 民間企業等

国内各地で演習

サイバーコロッセオ
cyber colosseo

(東京2020大会に向けた人材育成)

チケット販売

社会インフラ

公式HP

放送環境

WiFi・通信環境

避難・誘導

擬似オリンピック
ハラリンピック
システム

Attack! Guard!

＜準上級＞攻防戦を主体とした
実践的な演習プログラム

＜事業の対象範囲＞

- ・東京2020組織委員会及び業務受託ベンダー担当者
- ◆セキュリティソリューションを提供するベンダー等
- ◆システム全体の基盤となるネットワーク、プラットフォーム、大会競技システム等
- ◆広報・公式サイト、マーケティング・チケットサイト等

初級 中級 準上級

受講者のレベルに応じた
コロッセオ演習コースと
幅広い講義演習群
コロッセオカレッジ

2017 2020

220名以上

段階的強化

セキュリティイノベーターの育成

セックハックサンロクゴ
SecHack365

若手セキュリティイノベーター
育成プログラム

セキュリティの未来を生み出すU-25ハッカソン

先端科学技術
企業の見学

最先端技術の体験

海外派遣

全国の一流の
研究者・技術
者との交流

ハッカソン

学生講座

遠隔開発実習

修了生コミュニティ

発想力・研究・開発力の向上

アイデアソン・
ハッカソンイベント

開催地を変えて複数回実施
し、継続的に開発指導

豊富な研究資産

研究開発のノウハウ、
攻撃データ等の活用

オンラインでの指導・
遠隔開発実習

自宅などの遠隔地から
開発環境へアクセス可能

受講生への支援

長時間の学業との両立に
ついての助言、指導

最先端技術の体験

先端企業の見学による
社会体験で発想力を強化

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

2020年度コース概要

受講者の習熟度に応じて**Aコース及びBコースを開催**

- ◆ 事前オンライン学習（1時間程度）
- ◆ 実機演習・グループワーク（1日間）

年間100回程度開催、3,000人以上の受講が可能

- ◆ 全国47都道府県、100回程度開催
- ◆ 重要社会基盤事業者、民間企業等は、受講料を徴収（70,000円/人（税別））

CYDER受講者数の推移（累積数）



2020年度実施内容および対象組織

コース	難易度	主な対象組織	主な対象者	開催予定地	開催回数
Aコース (初級)	CSIRT アシスタント レベル	(全組織共通)	情報システムに携わる全ての方／ CSIRT要員／安全に情報システムを 運用したい方	47都道府県	65回
B-1コース (中級)	CSIRT メンバー レベル	地方公共団体向け	CSIRT要員、インシデント発生時に 対応要員となる方／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	全国11地域	20回
B-2コース (中級)		国の機関（28組織）、独立行政法人等（87法人）、 指定法人（9法人）、重要社会基盤事業者（14分野※）、 民間企業等向け		東京・名古屋 大阪・福岡	15回

●上記以外に、難易度や受講環境の異なるコースを検討中

※14分野：情報通信、金融、航空、空港、鉄道、電力、ガス、医療、水道、物流、化学、クレジット、石油 等

※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

✓ 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

✓ 攻撃・対処シナリオ

現実起きたサイバー攻撃の最新事例を踏まえ、コース別に異なるシナリオを準備。繰り返し受講することにより、様々な攻撃に対する対処法を学ぶことが可能

演習シナリオ例

Aコース (2019年度)

- ① 標的型攻撃メールを受信した株式会社サイダーの職員が、添付されていたドキュメントファイルを開いて、マルウェアに感染
- ② その職員の端末から社内の他の端末へ感染が拡大

B-1コース (2019年度)

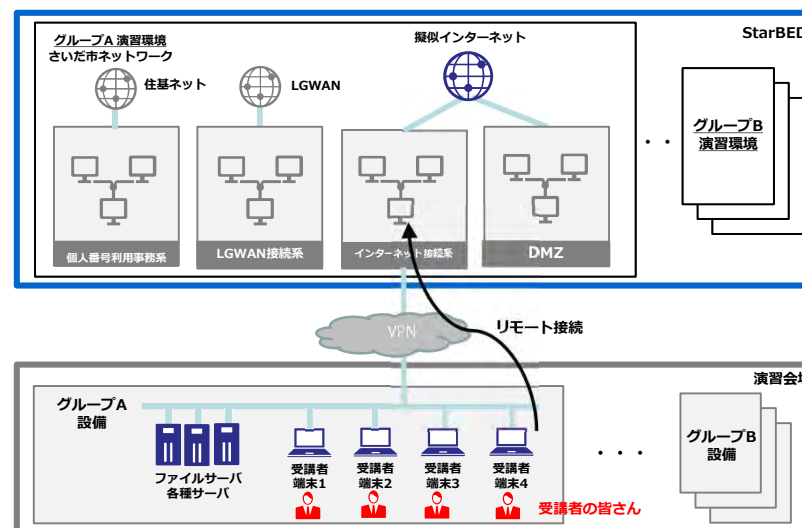
- ① CMS (コンテンツ・マネジメント・システム) の脆弱性を用いて侵入・改ざんされたWebサイトにさいだ市の職員がアクセスした結果、マルウェアに感染
- ② その職員の端末から、庁内システム内にマルウェア感染が拡大、機密ファイルが漏洩しメールサーバーにマイニングツールが設置される

B-2コース (2019年度)

- ① さいだ省の職員が、悪意のある広告 (マルバタイジング) を含んだ一般のニュースサイトにアクセスし、マルウェアに感染
- ② その職員の端末から、省内システム内にマルウェアが感染拡大、機密ファイルが漏洩する

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



インシデント発生から解決、事後対応までを体験



- ✓ コロナ禍における緊急的な措置及びCYDERの周知啓発の取組の一環として**Webで教材を無料提供**
- ✓ 申込総数は**4,624件**（一般公開期間：5/12～6/30）
- ✓ CYDERの本来のターゲットである国の機関等及び地方公共団体の申込は17%程度にとどまったものの、複数の組織から申込があり、国内における**CYDERの需要の高さ**が明確となった

組織種別	申込み組織数	申込数	割合
国の機関(28組織)	18組織	170	3.8%
独立行政法人(87組織)	37組織	102	2.3%
指定法人(9組織)	5組織	12	0.3%
地方公共団体(1,788組織)	409組織	494	11.1%
重要社会基盤事業者	843組織	1,561	35.2%
民間企業	353組織	638	14.4%
学校	794組織	1,206	27.2%
個人	—	256	5.8%
総計		4,439	100%

申込総数：4,624件 エラー/重複申込数※：185件 ※上記表の数値に含まず

申込み理由（複数回答）	回答数	割合
CYDER演習がどのようなものなのか試してみたかった	2,673	60.2%
組織内のセキュリティ研修に役立ちそうだったので	2,634	59.3%
自宅で学習できるので	1,158	26.1%
インシデントハンドリングを学んだことがないから	1,093	24.6%
過去にCYDERを受講し、復習したいと思ったので	421	9.5%
組織で過去にインシデントが発生したがうまく対処できなかったため	191	4.3%
その他	231	5.2%

●その他の回答

・自己啓発のため（58）

・業務に役立ちそうだったので（27）

・社内/学内教育に役立てたい（18）

・サイバーセキュリティに関心がある（24）

・CYDER受講できない・できなかったため

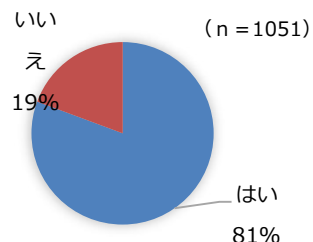
・社内/学内からの紹介

・CYDERの予習/復習、受講促進のため

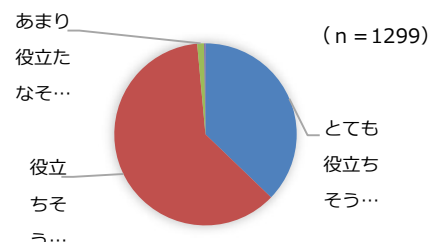
・在宅勤務のセキュリティ対策

・無料だったので

今後CYDERに参加してみたいと思いましたか？



この教材は役立ちそうですか？



CYDERへの興味関心についてご回答ください。（複数選択可）

1	（自分が）参加したいと思う。	547
2	部下・同僚に参加させたいと思う。	394
3	教材を読むだけでは物足りないと感じたので、CYDERに参加したい	188
4	自組織ではグループ演習の実現が難しいので、CYDERに参加したい	179
5	参加したいが、外部の研修に行かせて貰えない	90

●その他の回答

・お客様に参加して貰いたい。

・オンラインでの受講が可能であれば参加したい

・過去に参加している

・できれば参加してみたいが、業務が忙しい...

・組織に属していないため参加できない

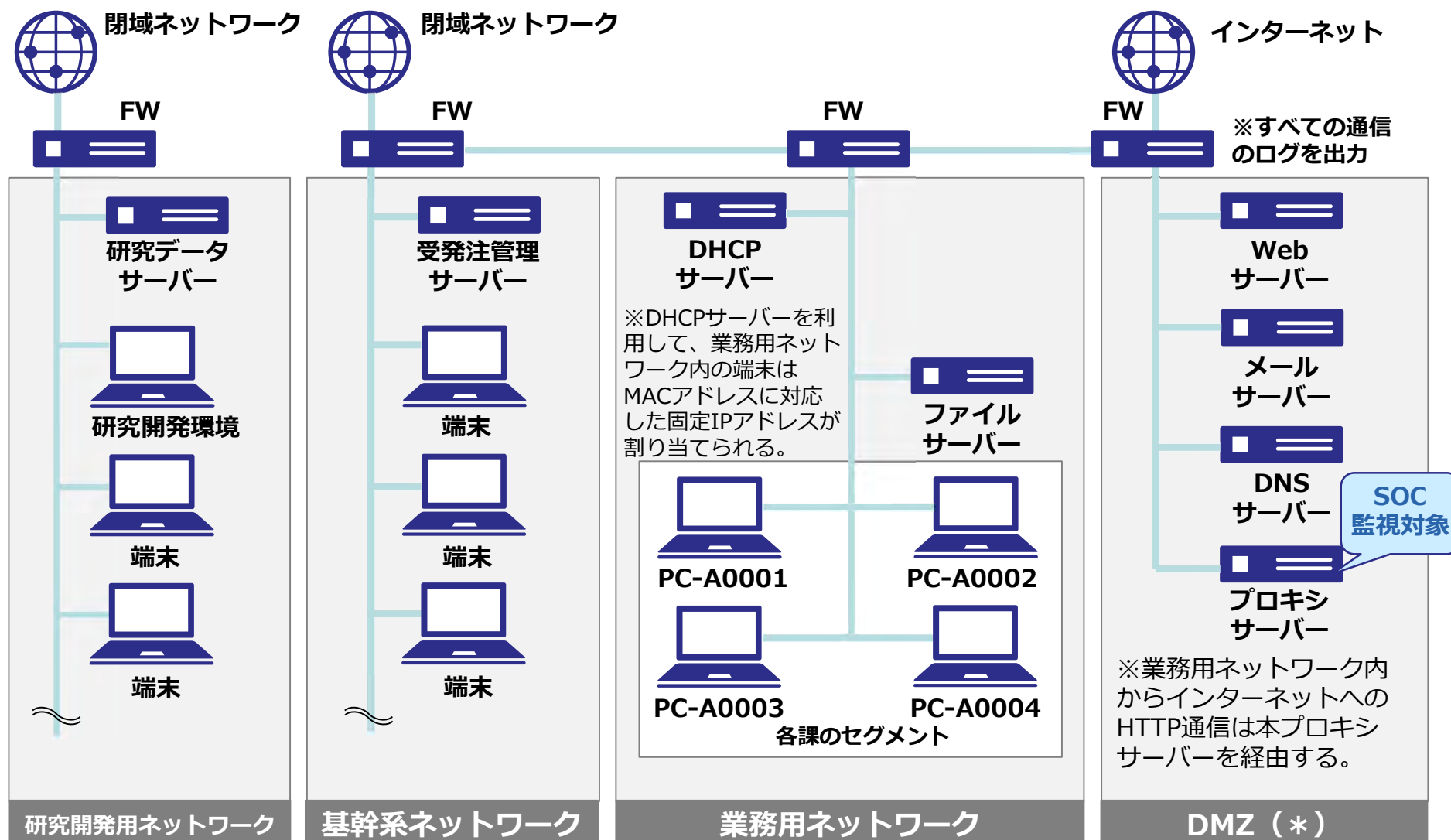
・上長へ相談して検討したい

・民間企業勤務のためコスト面で難しい。

プレスリリース：実践的サイバー防御演習「CYDER」の教材を期間限定で一般公開 <https://www.nict.go.jp/press/2020/05/12-1.html>

[デモ]
演習説明資料 2020 年 A コース

実習舞台設定（LAN）



(*) DMZ (DeMilitarized Zone) : 外部（インターネット）との通信を直接行う機器のみを設置したネットワーク領域のこと。外部との通信を直接行う機器をDMZのみに配置し、組織内部の機器と外部の直接の通信を禁止することで、組織内部のネットワークの安全性を高めることができる。

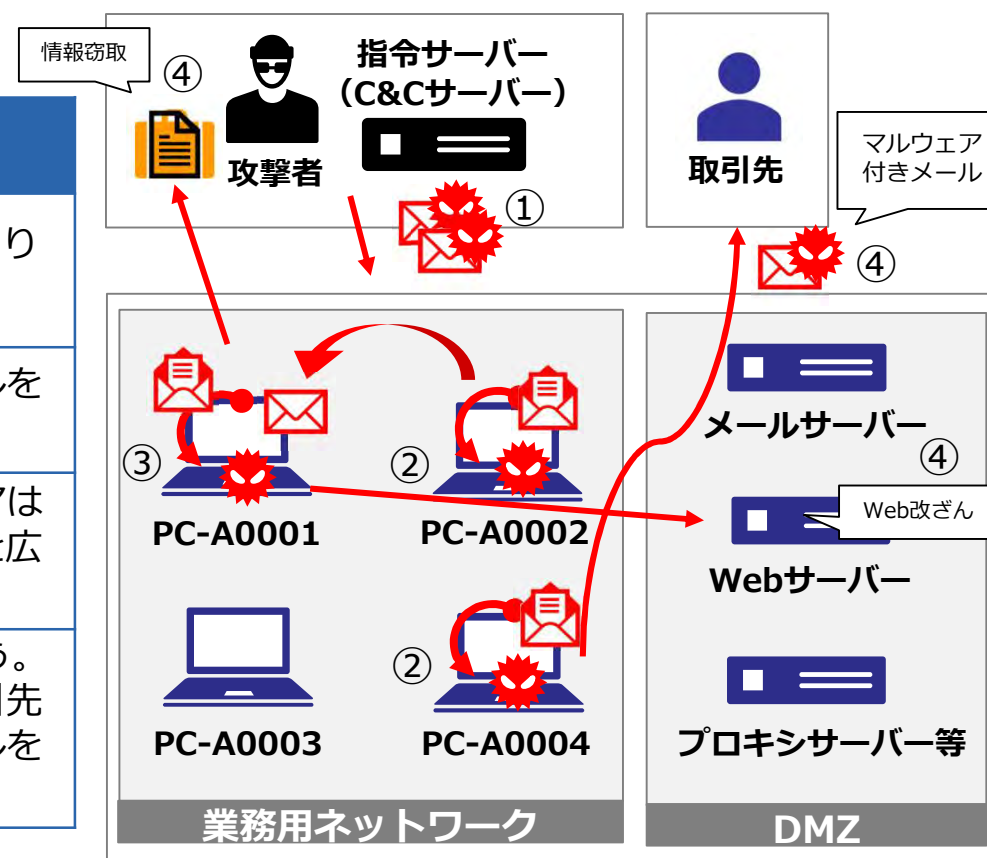
A コース攻撃シナリオ概要

• テーマ (あらすじ)

- 攻撃者は株式会社サイダーの複数社員に、なりすましメール(Emotet)を送付する。メールを受信した一部の社員がメールの添付ファイルを開き、社員端末がマルウェアに感染する。社員端末に感染したマルウェアはその他の端末にメールで感染を広げ、攻撃者がマルウェアと指令サーバーを使って情報の窃取やWeb改ざんを行う。さらに、マルウェアに感染した社員端末から取引先企業へ、マルウェア付きのメールが送付される。

• 攻撃の主な流れ

#	主体	事象概要
①	攻撃者	(株)サイダーの複数社員へ、なりすましメール(Emotet)を送付
②	社員	受信したメールの添付ファイルを開き、マルウェアに感染
③	攻撃者	社員端末に感染したマルウェアはその他の端末にメールで感染を広げる
④	攻撃者	情報の窃取やWeb改ざんを行う。さらに、(株)サイダーの取引先企業へマルウェア付きのメールを送付



事案対応の流れ

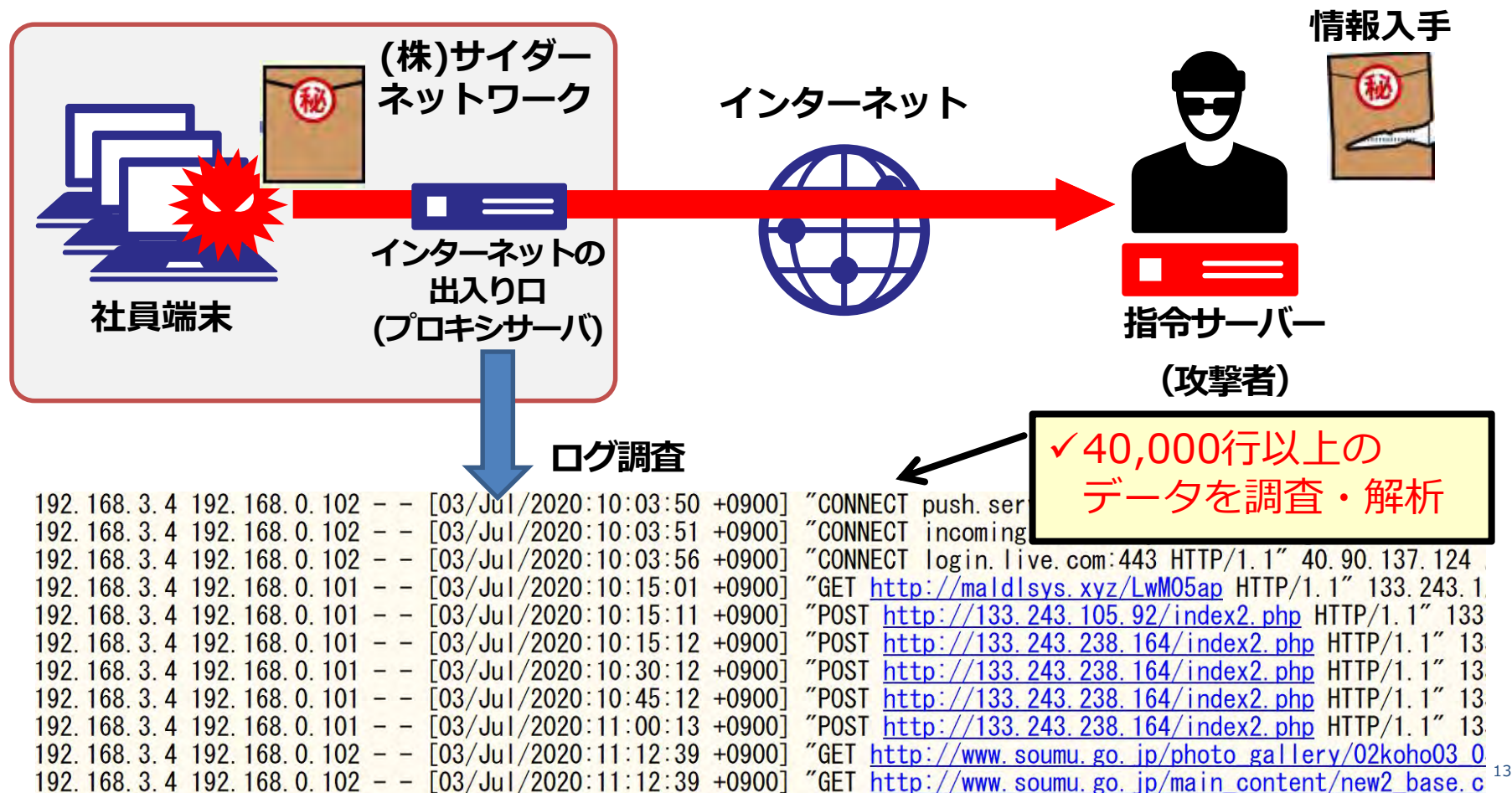
課題	インシデント対応フェーズ	概要
1	検知・受付・トリアージ・対応方針の検討	発生している事象に対する対応の優先度付け
2	証拠保全	インシデントに関する証拠の保全
3	封じ込め・根絶	影響範囲の特定と対応方針の検討
4	復旧措置（暫定対応）・再発防止（恒久対応）	インシデント収束に向けた対応の検討
5	報告・公表	報告書作成

デモ

[ポイント]マルウェア感染端末および利用者特定のため、プロキシサーバーのログを分析

事実確認 (プロキシログの調査)

マルウェア感染端末および利用者特定のため、提供された指令サーバーの情報をもとに、インターネットアクセスに関するログと、端末管理台帳を検索します。



ログの詳細



検索条件 "133.243.105.92"
検索対象 *.*
フォルダ C:¥Users¥cyberuser¥Desktop¥Aコース¥課題3

```
192.168.3.4 192.168.0.101 - - [03/Jul/2020:10:15:11 +0900] "POST http://133.243.105.92/index2.php" 404
192.168.3.4 192.168.0.101 - - [03/Jul/2020:13:35:21 +0900] "POST http://133.243.105.92/index2.php" 404
192.168.3.4 192.168.0.103 - - [03/Jul/2020:14:25:16 +0900] "POST http://133.243.105.92/index2.php" 404
192.168.3.4 192.168.0.104 - - [06/Jul/2020:09:55:43 +0900] "POST http://133.243.105.92/index2.php" 404
192.168.3.4 192.168.0.101 - - [06/Jul/2020:10:10:41 +0900] "POST http://133.243.105.92/index2.php" 404
192.168.3.4 192.168.0.103 - - [06/Jul/2020:10:10:52 +0900] "POST http://133.243.105.92/index2.php" 404
192.168.3.4 192.168.0.104 - - [06/Jul/2020:10:55:43 +0900] "POST http://133.243.105.92/index2.php" 404
```

プロキシサーバーのログを調査することで、IPアドレス「192.168.0.101」の端末などから、通信が発生していることがわかります。

端末名	IPアドレス	デフォルトゲートウェイ	設置セグメント	利用者	利用者所属(部)
PC-A0001	192.168.0.101	192.168.0.253	営業部セグメント	亀井 晴信	営業部
PC-A0002	192.168.0.101	192.168.0.253	営業部セグメント	野村 淳子	営業部
PC-A0003	192.168.0.102	192.168.0.253	営業部セグメント	多田 暉一郎	営業部
PC-A0004	192.168.0.103	192.168.0.253	営業部セグメント	金井 敏	営業部

端末管理台帳からIPアドレス「192.168.0.101」の端末は、インターネット接続系にある端末「PC-A0002」であることがわかります。

- 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に対し、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能力を有するサイバーセキュリティ人材を育成。最終的に約220人以上のセキュリティ担当者等を育成予定

2020年度コース概要

コロッセオ演習

受講者の習熟度や業務の性質等に合わせて、**初級・中級・準上級コースを設定**

- ◆事前オンライン学習
- ◆高度セキュリティ講義演習（準上級のみ）・実機演習・グループワーク
- ◆オンライン復習

コロッセオカレッジ

コロッセオ演習と連携する**20科目の講義演習（選択受講制）**

2020年度実施内容および対象組織

コース		難易度	対象組織	開催地	開催回数
コロッセオ演習	初級コース	CSIRTアシスタントレベル	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	東京	Aコース1回 Bコース1回
	中級コース	CSIRTメンバーレベル			Aコース1回 Bコース2回
	準上級コース	データ解析者レベル			Aコース2回 Bコース1回 Cコース2回
コロッセオカレッジ					20科目

※サイバーコロッセオは、(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

15

コロッセオ演習

➤ 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模擬して構築

➤ 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

ー 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



コロッセオカレッジ

- コロッセオ演習内でカバーできない、かつ 東京2020大会開催に必要と思われる広範な 講義演習
- 選択受講制
 - ー 受講者が自身のスキルマップに基づき不足している領域の講義演習を選択

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

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)

特長

豊富な研究資産
NICTの知見・人的資源、研究開発のノウハウ、攻撃データ等の活用。

最先端技術の体験
先端企業の見学による社会体験で発想力を強化。講演を聞く事でプレゼンテーションスキルアップにつなげる。

アイデアソン・ハッカソンイベント
開催地を変えて複数回実施し、継続的に開発指導。オフラインで議論、検討、相談、発表を行う。

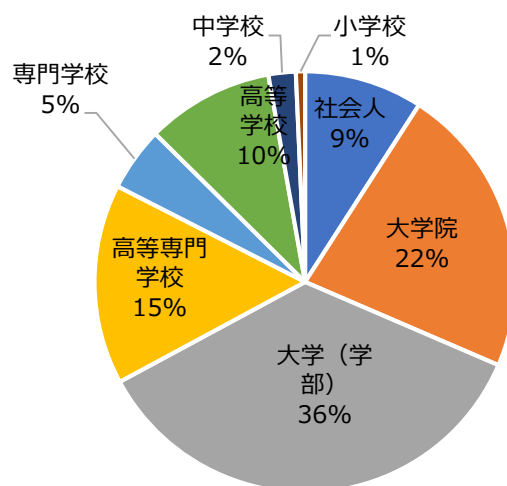
受講生への支援
長期間の学業との両立についての助言、指導。作る→見せるを習慣化し作品のイメージを早期に具体化。

オンラインでの指導・遠隔開発演習
自宅などの遠隔地から開発環境へアクセス可能。チャットやタスク管理ツールを活用した持続的な指導を実施。

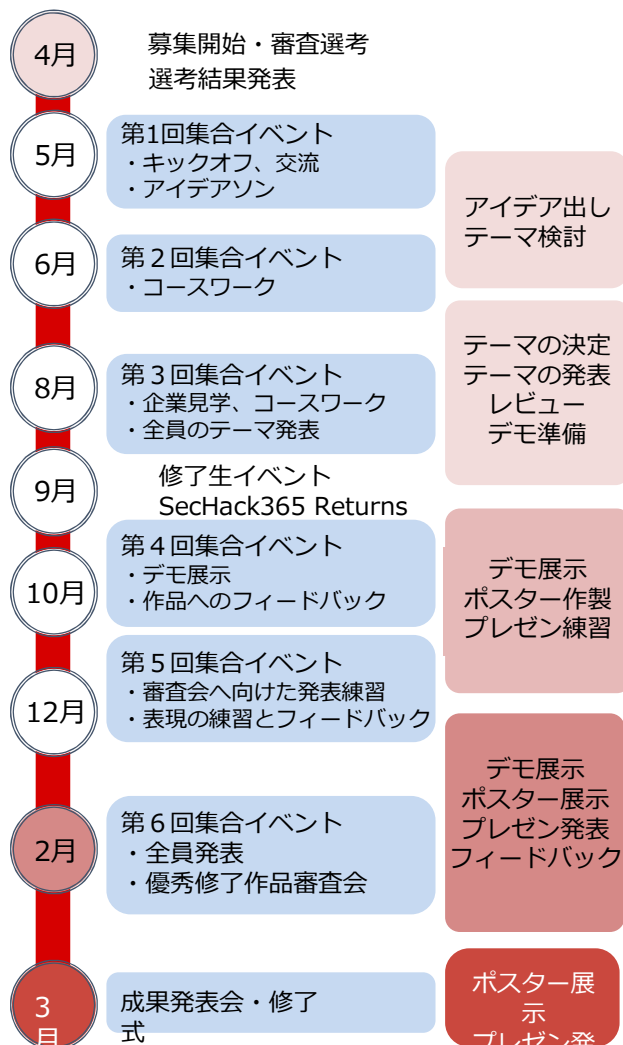
年間プログラム例 (2019年度)



受講生属性 (2017～2019年度)



1年間のプログラム例

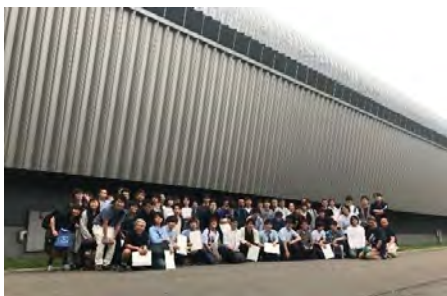


コース概要

- 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。

表現駆動 コース	- アイデアを形にする過程で価値を最大化するなど、サービスを磨き上げるコース - グループでのハッカソン実施により、サービスづくりを進める
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を進めるコース - 付加学習により、他の技術や他分野を知ること、作るもののアイデアの幅を広げる
開発駆動 コース	- 開発することに重きをおいて、開発指導に特化したコース - 定まっている開発テーマや分野について指導を受け、開発を進める
思索駆動 コース	- 問題を発見して、その問題を深く理解した上で解決策の提案を試みるコース - 問題の発掘、鮮明化、解決手法の導出・設計・実装のプロセスを実施する
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 - 将来のセキュリティ分野における研究者になるため、研究者に必要なスキルを磨く

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



SCIS2020 暗号と情報セキュリティシンポジウム参加

電子情報通信学会・情報セキュリティ研究専門委員会主催
暗号と情報セキュリティ技術に関する最新の研究成果を発表し、情報交換の場を提供する場となっている。

【研究コース】中田 有哉 (大学院生)

日時 : 2020年1月28日(火)~30日(木)

発表内容: 「ネットワーク間の協調による
DRDoS攻撃対策手法」

目的 : SecHack365受講生として、開発
の成果をネットワークセキュ
リティ技術分野の研究者や専門家が
集まる会合にて発表。



JANOG (Japan Network Operators' Group) ミーティング参加

日本ネットワークオペレーターズグループ主催
北米ネットワークオペレーターズ・グループ) の日本版。日本のインターネット
に於ける技術的事項やオペレーションに関する事項を議論、検討、紹介。

【学習コース】灰原 渉 (大学生)

日時 : 2020年1月22日(水)~24(金)

発表内容: 「Sereform SF: IoT機器として
のSoC FPGAを遠隔から自由に操
作するための、締め付けないセ
キュリティ基盤」

目的 : SecHack365受講生としての研
究開発の成果をネットワーク運
用事業の専門家が集まる会議で
発表。



開発作品「光るLANケーブル イルミパケット (ILLUMIPACKET)」を発表

【学習コース】麻生 航平 (大学院生)

SecHack365がスポンサーとなっている「SECCON2020」ではワーク
ショップを開催し、満員となった。好評のため企業数社から展示引き合い
があった。その他『セキュリティ博物館プロジェクト』にも参加。オーブ
ンソースカンファレンスでもデモを行った。

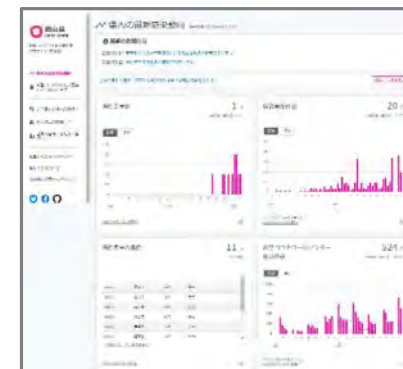


「岡山県の新型コロナウイルス感染症対策サイト（非公式）」の 立上げ

【学習コース】藤原 出帆 (高校生)

地元の岡山県が公開している新型コ
ロナウイルスの情報をわかりやすく
発信。

東京都のサイトを参考に、岡山県版
を約18時間で作成。現在は小学生・
中学生のエンジニアも含め、県内外
6人のボランティアで運営している。
ネットニュースや、地元のオンライ
ン新聞などに掲載された。



修了生コミュニティの活動

「SecHack365 Returns 2019」

日時 : 2019年9月28日(土)
会場 : 秋葉原コンベンションホール
参加者 : 2017年度修了生16人
2018年度修了生25名、合計41名
内容 : 若手研究者の講演、修了生の活動報告、
修了生企画、奨励賞表彰等



修了生発表	タイトル	
SecHack365 奨励賞	「サイバー攻防体験学習ゲームCyshipの成果発表」	2017年度修了生 Cyshipチーム (北村 拓也、友利 奈緒、川島 一記)
修了生 活動報告	「SXSW訪問で感じた世界に広まるサービスを作る方法」	2018年度修了生 秋田 賢
	「秘密計算技術の可能性と実装」	2017年度修了生 澤 佳祐
	「普通の大学院生が授業つくってみた -バグハンティングコンテストに寄せて-	2018年度修了生 古川 菜摘
	「SecHack365が教えてくれた」	2017年度修了生 三須 剛史
	「ExGDBの新機能とその他SecHack365以降の成果」	2018年度修了生 宮川 大星
	「米国で行われるCanSatの打ち上げ実験 ARLISSに参加してきた」	2018年度修了生 山本 悠介

修了生への機会の提供

サイバーテック・東京 (2019年11月26日～27日)

サイバーテック・テルアビブ (2020年1月28日～30日)

開催地 : 東京、テルアビブ (イスラエル)
参加者 : 【東京】修了生2名 (小松 聖矢、山本 悠介)
【イスラエル】修了生3名 (小松 聖矢、赤間 滉星、柴崎 研治)
がビデオ発表形式で参加
参加目的 : イスラエル国家サイバー総局と総務省とのMoC (MEMORANDUM OF COOPERATION) に基づき、両国間の人材育成協力の一環として世界的なサイバーセキュリティ関係のイベントに参加
世界の専門家を前にして発表の機会を提供

小松 聖矢	Analysis of Botnet Cooperative Behavior using Deep Learning on Darknet 「ダークネットにおける深層学習を用いたボットネット協調動作の解析」
赤間 厚生	Development of Buckler for sharing security signature 「『Buckler』探知機のシグネチャと判定するプログラムを分離するためのフレームワーク」
柴崎 研治	Support system for static analysis of malware using CNN 「マルウェア解析補助システム」



サイバーテック・グローバル

サイバー分野におけるB2Bネットワーキングプラットフォーム
テルアビブ、ローマ、東京、シンガポール、パナマなど世界の都市でサイバー分野における最新のテクノロジーイノベーション、脅威やソリューションなどを紹介する場として開催

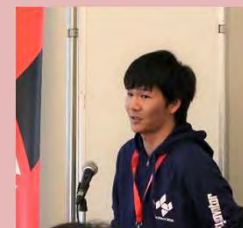


2017年度優秀修了生 北村 拓也 さん (受講時：大学院生)



- ・ 未踏IT人材発掘 育成事業採択 (2017年度)
- ・ 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)
- ・ MAKERS UNIVERSITY第3期生
- ・ 『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 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/>)

2017年度優秀修了生 室田 雅貴 さん (受講時：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
- ・ MAKERS UNIVERSITY第4期生

2017年度修了生 市川 友貴 さん (受講時：大学生)



- ・ 未踏IT人材発掘 育成事業採択 (2019年度)
- ・ 学生クリエイター支援クマ財団2期生・3期生
- ・ Todai To Texas 2020 DemoDayAward 受賞
- ・ 未踏IT人材発掘・育成事業スーパークリエイター認定 (2019)

2017年度修了生 ニノ方 理仁 さん (受講時：小学生)

- ・ ITスーパーエンジニア・サポートプログラム “すどうで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年度優秀修了生 朱 義文 さん (受講時：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 - 手で作る組み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
- ・ 東京都私学財団「文化・スポーツ活動賞」受賞

2018年度修了生 窪田 靖之 さん (受講時：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 (受講時：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

NICT 第 5 期中長期計画における事業方針

受講対象組織への調査

全ての国の機関等・地方公共団体を対象（1,911組織）としたアンケート調査を実施

※2019年10月に実施
回答率47%

調査
結果

公的機関においてサイバー演習を受講
すべき**セキュリティ担当者**の人数

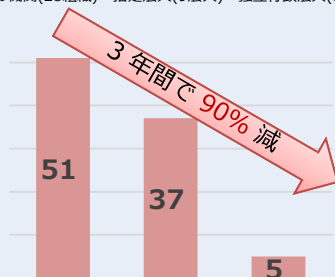
約 **6,200人**

人事異動（2～3年）を考慮すると、
年3,000人規模の育成が継続的に必要

未受講組織の低減に向けた取組

➤ 未受講組織数（H29年度以降も受講したことがない組織の数）

国の機関等（124組織）
※国の機関(28組織)・指定法人(9法人)・独立行政法人(87組織)



H29年度 H30年度 R1年度

地方公共団体（1,788団体）



H29年度 H30年度 R1年度

➤ 未受講理由

国の機関等・地方公共団体
を対象にした2019年10月
の調査結果（上位5つ）

業務多忙	235
開催場所が遠い	145
開催日程が合わない	99
難易度が高すぎる	85
CYDERを知らなかった	70

受講促進の取組

➤ 周知広報

受講対象組織へのパンフレット送付、セ
キュリティイベントへの出展等を実施

➤ 演習日程・開催場所の調整

各都道府県の自治体職員が受講しやすい日
程・場所について、都道府県庁や総務省の
総合通信局等に聴取し、スケジュールに反
映

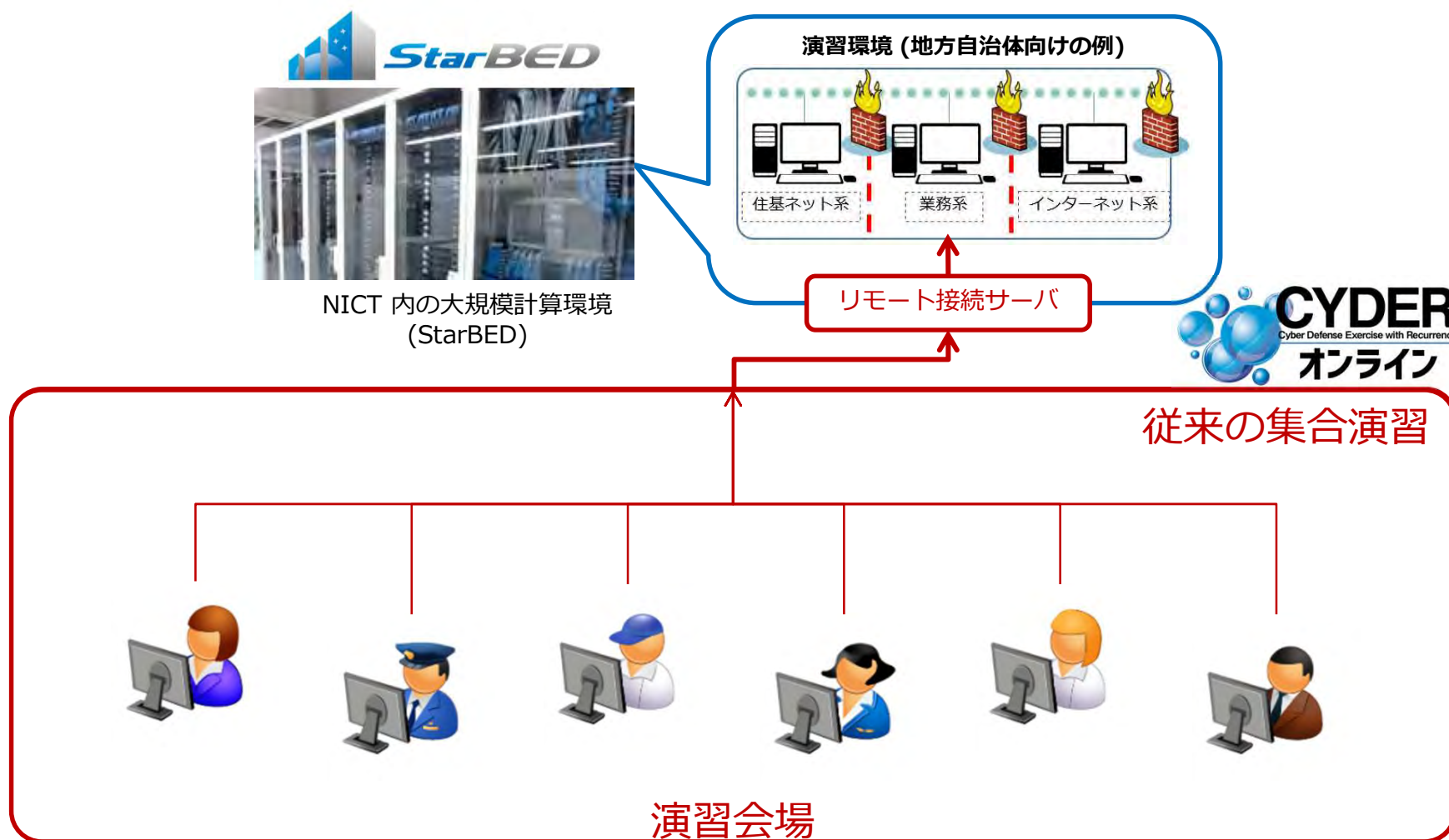
➤ 都道府県を通じた受講計画策定

総務省（サイバーセキュリティ統括官室及
び地域情報政策室）から都道府県に対し、
傘下の市町村に対するCYDER受講計画を策
定し、受講を促すよう事務連絡にて依頼

➤ オンライン演習環境の整備

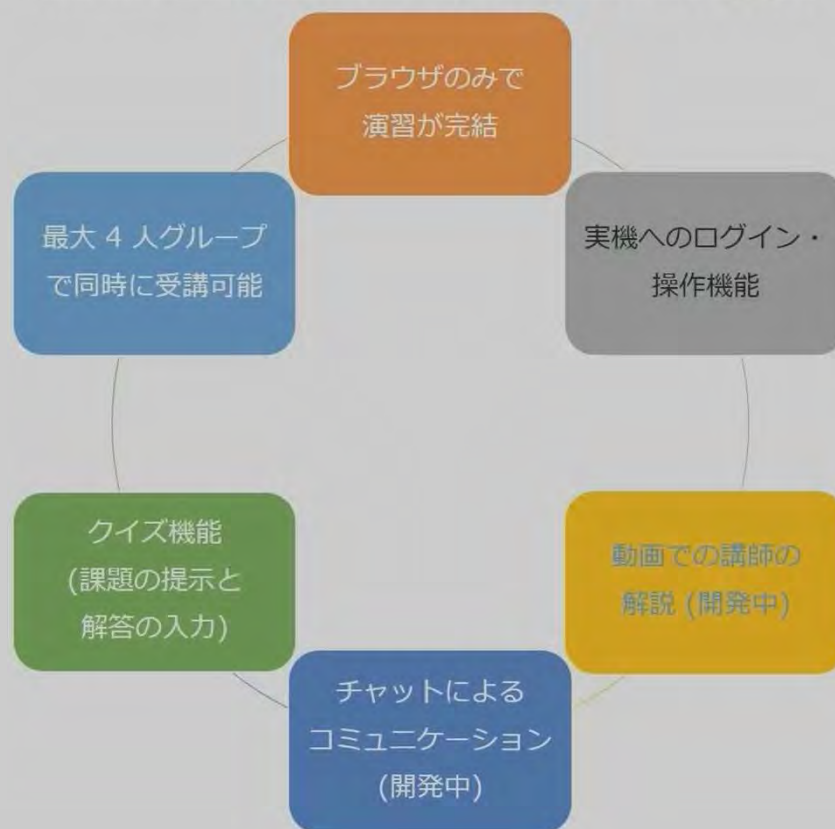
オンラインで演習が可能となる演習コース
を令和3年度より運用予定
（令和3年1～3月に試験運用を実施）

CYDER の未受講組織の低減と新たな生活様式に対応するため、完全オンラインで**実機演習**を体験可能な演習環境を **R2 年度より段階的に提供開始**。受講者は自組織のパソコンの **Web ブラウザ**を利用して、NICT 内の大規模演習環境に接続し、実践的な演習を受講可能。

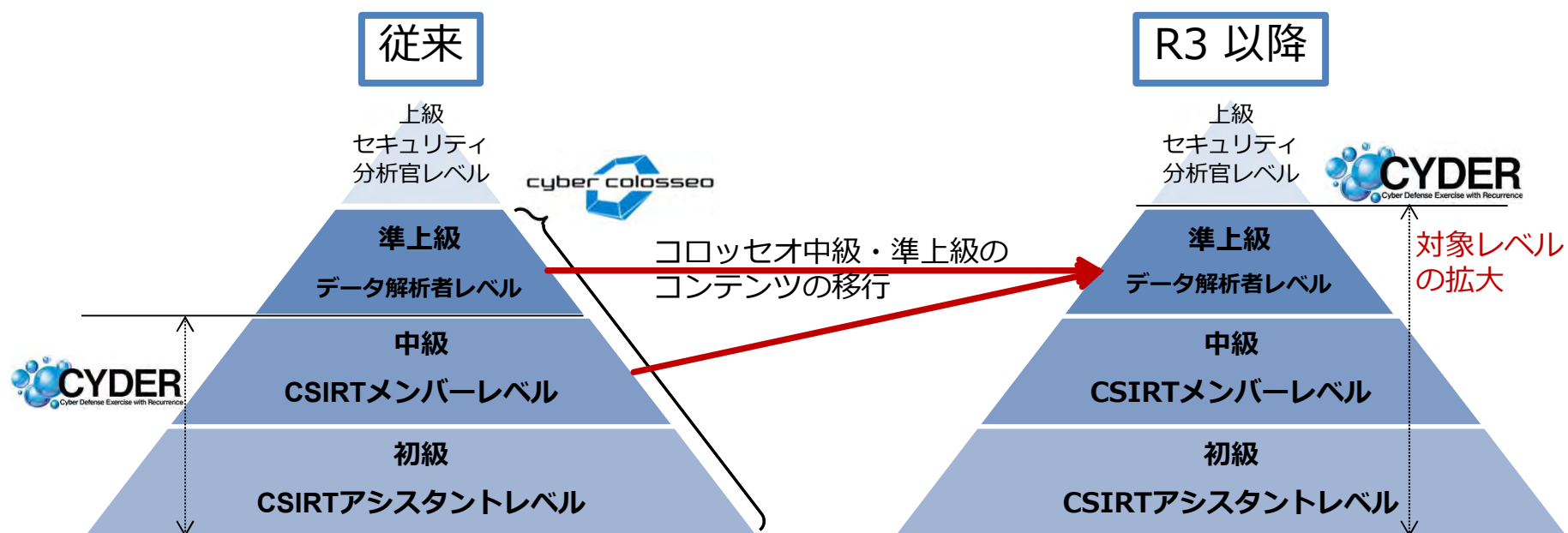


○実機オンライン演習システム (オンライン版 CYDERANGE) の**デモ動画**をご覧ください。

オンライン版 CYDERANGE の主な機能



- ✓ R2 年度をもって事業が終了したサイバーコロッセオの演習コンテンツを活用し、R3 年度に「**CYDER C (準上級)**」コースを新設予定。



● 2021年度 実施の基本方針 ●

- ✓ 2020年度と同様に新型コロナウイルス対応のため**オンラインを基本**にした実施を検討
- ✓ **イベントを6回、成果発表会を1回、Returnsを1回**での実施とする。
- ✓ **人数規模は例年と同程度** (トレーニー 40 名、外部トレーナー 20 名程度)

・ 主要イベント

4月に募集開始、2ヶ月に1回程度の頻度でオンラインイベントを実施

- 5月回：顔合わせ・キックオフ
- 7月回：活動状況の把握と助言
- 8月回：テーマ発表
- 10月回：作品デモ展示・ポスター発表
- 12月回：最終発表への練習と助言
- 2月回：最終発表

・ それ以外のイベント実施

- 9月：SecHack365 Returns
- 3月：成果発表会

・ オンライン指導

集合回以外の期間にトレーナーがオンラインで指導。オンラインイベントを合わせて実施して、講義や講演などの追加指導を実施。



SecHack365
SECURITY・HACKATHON 365 DAYS

Change the World

サイバーセキュリティで世界を変えよう

一生モノの365日が、ここにある。

SecHack365 公式サイトを
チェック

25歳以下を対象に、セキュリティノバターとなる若手を育成

SecHack365とは、「SECURITY・HACKATHON 365 DAYS」を意味する名称で、25歳以下を対象に、セキュリティマインドを持ち、革新的な研究・開発ができるセキュリティノバターを育成する民間ハッカソンです。

国立研究開発法人情報通信研究機構(NICT)の持つ研究資産を活用しながら、一年をかけて実践的な研究・開発に取り組めます。

🔍 知る「技術」	🔍 知る「経験」	🔍 作る「仲間」
一線級の研究者・技術者による指導がオンラインで365日受けられます。 NICTならではの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して、開発をバックアップします。	365日のモノづくりは様々な経験の連続です。SecHack365では手を動かして作ることで、あらかじめ考えることが大切とされています。アイデアソン・ハッカソンイベントを年々回覧し、徹底してアウトプット型人材を目指します。	全国から集まった仲間との切磋琢磨の時間は学校では得られないものです。同じ時間を過ごした仲間とは、修了生として将来にわたってつながっていきます。もちろん多くの一線級のトレーナーとの出会いも待っています。

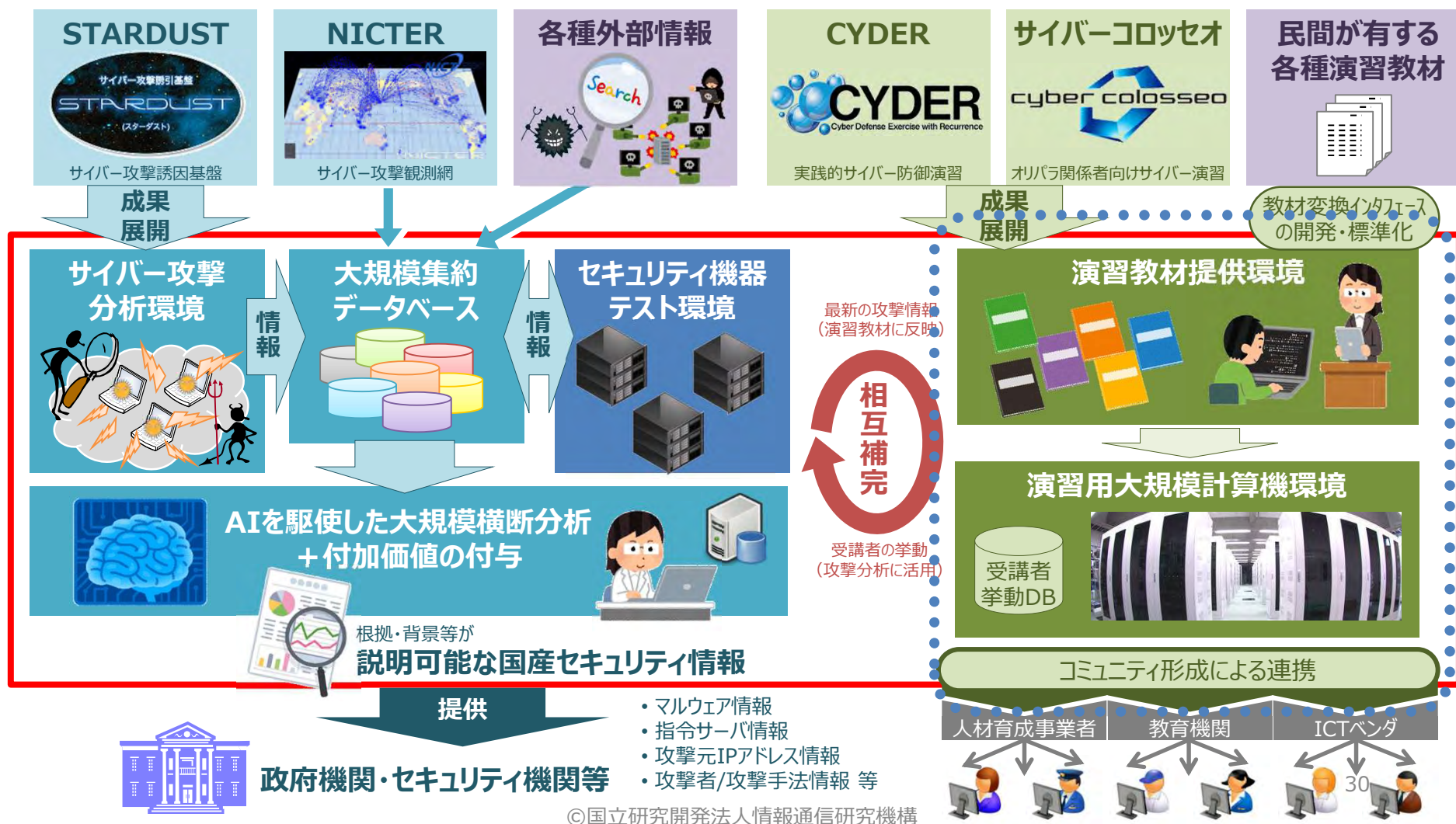
<https://sechack365.nict.go.jp/>

人材育成オープンプラットフォーム

サイバーセキュリティ統合知的・人材育成基盤



- サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤をNICTに構築し、産学の結節点として開放することで、サイバーセキュリティ対応能力の向上を図る。



セキュリティ人材育成に関する課題 (NICT による国内有識者へのヒアリング結果より)



- 人材育成事業の単独実施から**人材育成基盤・コンテンツのオープン化**により**地域や組織が自律的に活用できる社会へ**

我が国はサイバーセキュリティ自給率が他国に比べて低く、サイバー演習においても**海外製の演習環境やシナリオに依存**しがち。日本特有のインシデント事例等が活用されていないことが、**安全保障の観点において大きな課題**



民間の教育事業者

演習用の環境構築やシナリオ開発には高度な知識や技術力が必要となるが、これらに**単一組織だけで取り組む**のは非常に効率が悪いため共同開発体制が必要。それと並行して**教材フォーマット等の標準化**も重要

演習事業の実施にあたっては、その**基盤となる計算機環境や演習システム**が必要となるが、その構築と維持には高い技術力が必要であり、単一組織での構築・長期的運用は困難

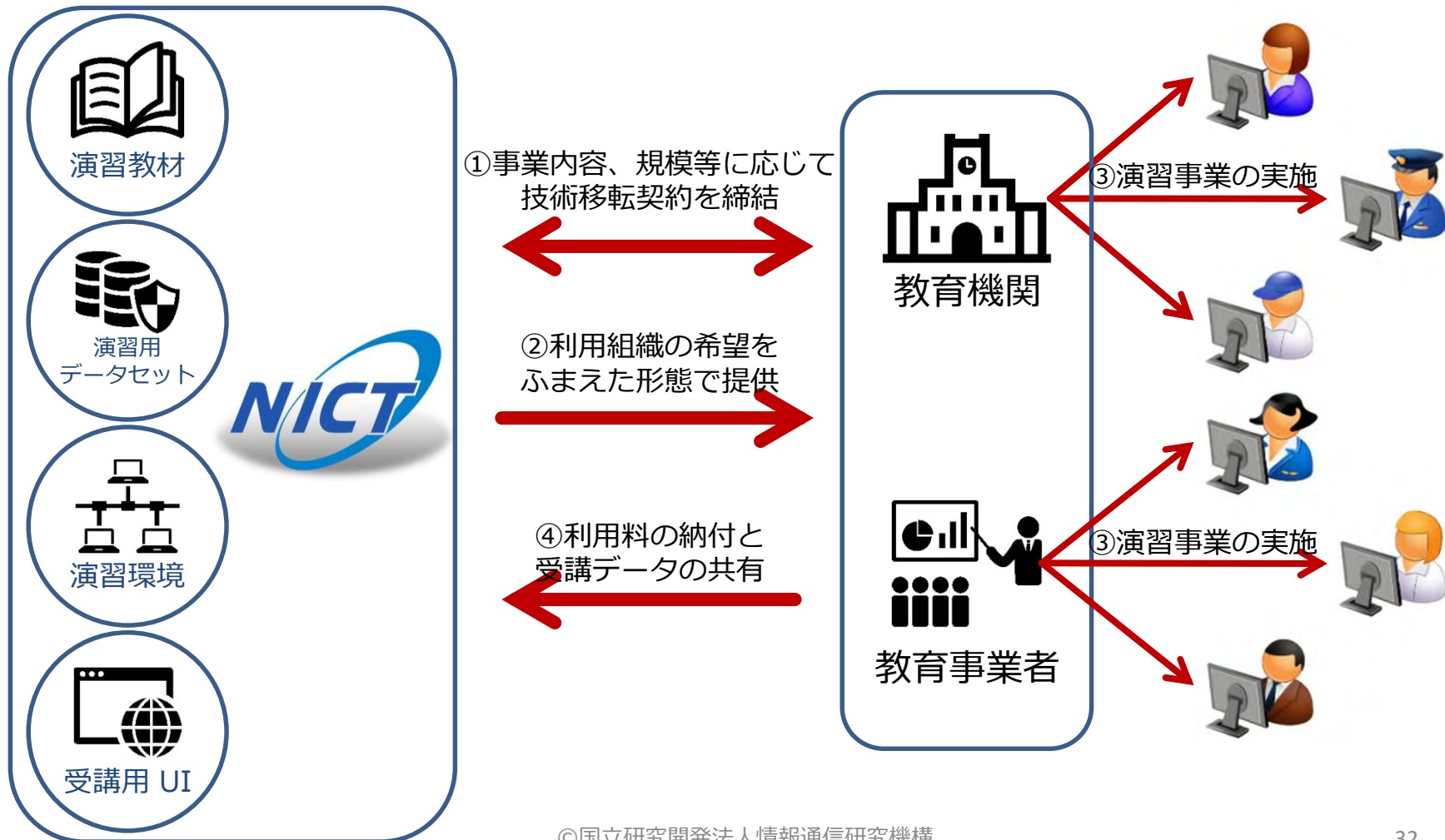


よりオープンな人材育成環境と協力体制の必要性

- ✓ 我が国ならではの**演習コンテンツ**開発体制の実現
- ✓ 各組織が持つ既存の**演習コンテンツの共有**や、相互活用と共同開発を実施
- ✓ 産学官の連携して**教材・環境の標準化**を進め、社会全体での開発効率を向上
- ✓ **基盤となる計算機環境**についても産学官が（相応の対価の下で）共同利用

人材育成オープンプラットフォームのサービス提供イメージ

- 利用希望組織は、事業内容、事業希望等に応じて、プラットフォーム利用のための技術移転契約を NICT と締結
- NICT は利用組織の希望をふまえて、演習教材、演習用データセット、演習環境、受講用ユーザーインターフェース (UI) 等のすべて、または一部を提供

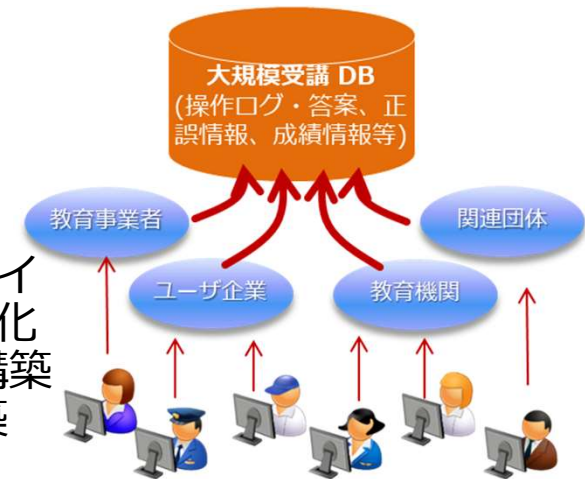


1. 人材育成コミュニティ（連携体制）の醸成

- ✓ 民間事業者や教育機関等のヒアリング（ユーザニーズ調査）
- ✓ 連携先機関が活用し易いライセンス形態の整理
- ✓ 大規模受講データベース等を活用した民間事業者や教育機関等との共同研究開発

2. 人材育成基盤の開発、構築

- ✓ 接続用API、オンライン演習用ユーザインターフェイス等のCYDERANGE（演習用ミドルウェア）の高度化
- ✓ 受講データを収集する大規模受講データベースの構築
- ✓ 演習用ミドルウェアを支える大規模計算環境の構築



3. 人材育成基盤利用促進のためのパイロットコンテンツ開発

- ✓ 既存コンテンツをベースに、よりユーザニーズに適合したパイロットコンテンツ（パイロットシナリオ・サンプルデータセット等）を開発
- ✓ 社会的な需要に応じ、システム構築技術者、システム開発者、一般の SOC 担当者等のセキュリティ対応力向上を目的としたコンテンツを開発予定

- 2016 年度の組織立ち上げ以降、 5 カ年にわたり、 CYDER、サイバーコロッセオ、 SecHack365 の 3 事業を推進
- セキュリティ人材育成に関わる課題は山積
 - 行政機関における演習受講率の低迷
 - 日本におけるサイバーセキュリティ自給率
 - 産学におけるセキュリティ人材育成の活性化
- 持続的なセキュリティ人材の供給に向けて



人材育成オープン
プラットフォーム