資料5－3

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

平成29年5月31日

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　センター長　園田　道夫

目次

１．組織概要

２．事業概要

　２－１．実践的サイバー防御演習（CYDER）

　２－２．サイバー・コロッセオ

　２－３．若手セキュリティエンジニア育成プログラム（SecHack365）

３．ナショナルサイバートレーニングセンターの今後の方向性

１．組織概要

１－１．ナショナルサイバートレーニングセンターの設置について

1-1.「ナショナルサイバートレーニングセンター」の設置について

○　我が国全体として、多様化・悪質化するサイバー攻撃に対抗し、社会の安全を守っていくためには、その担い手となるサイバーセキュリティ人材の育成を一層加速する必要。
○　ＮＩＣＴは、その研究成果や技術的知見を最大限に活用することにより実践的なサイバートレーニングを企画・推進する組織である「ナショナルサイバートレーニングセンター」を設置（H29.4.1）。

・国の行政機関、地方公共団体、重要インフラ等を対象とする実践的サイバー防御演習（CYDER）
　⇒　*47都道府県で演習を実施し、演習規模を100回3000人まで拡大*
・2020年東京オリンピック・パラリンピック競技大会の適切な運営に向けたセキュリティ人材の育成（サイバー・コロッセオ）
　⇒　*2020年東京大会開催時に想定される、IoTを含む高度な攻撃に対応した演習を実施*
・若手セキュリティエンジニアの育成（SecHack365）
　⇒　*25歳以下の若手人材を広く公募し、セキュリティの技術開発を本格指導*

【平成29年度総務省予算】ナショナルサイバートレーニングセンターの構築：15.0億円

実践的な防御演習

東京大会に向けた人材育成

若手セキュリティエンジニアの育成

「ナショナルサイバートレーニングセンター」

２－１．実践的サイバー防御演習（CYDER）

２－１－１．実践的サイバー防御演習（CYDER）

２－１－２．　CYDERの沿革・実績

２－１－３．平成29年度CYDER年間開催日程

２－１－４．平成29年度CYDER演習内容

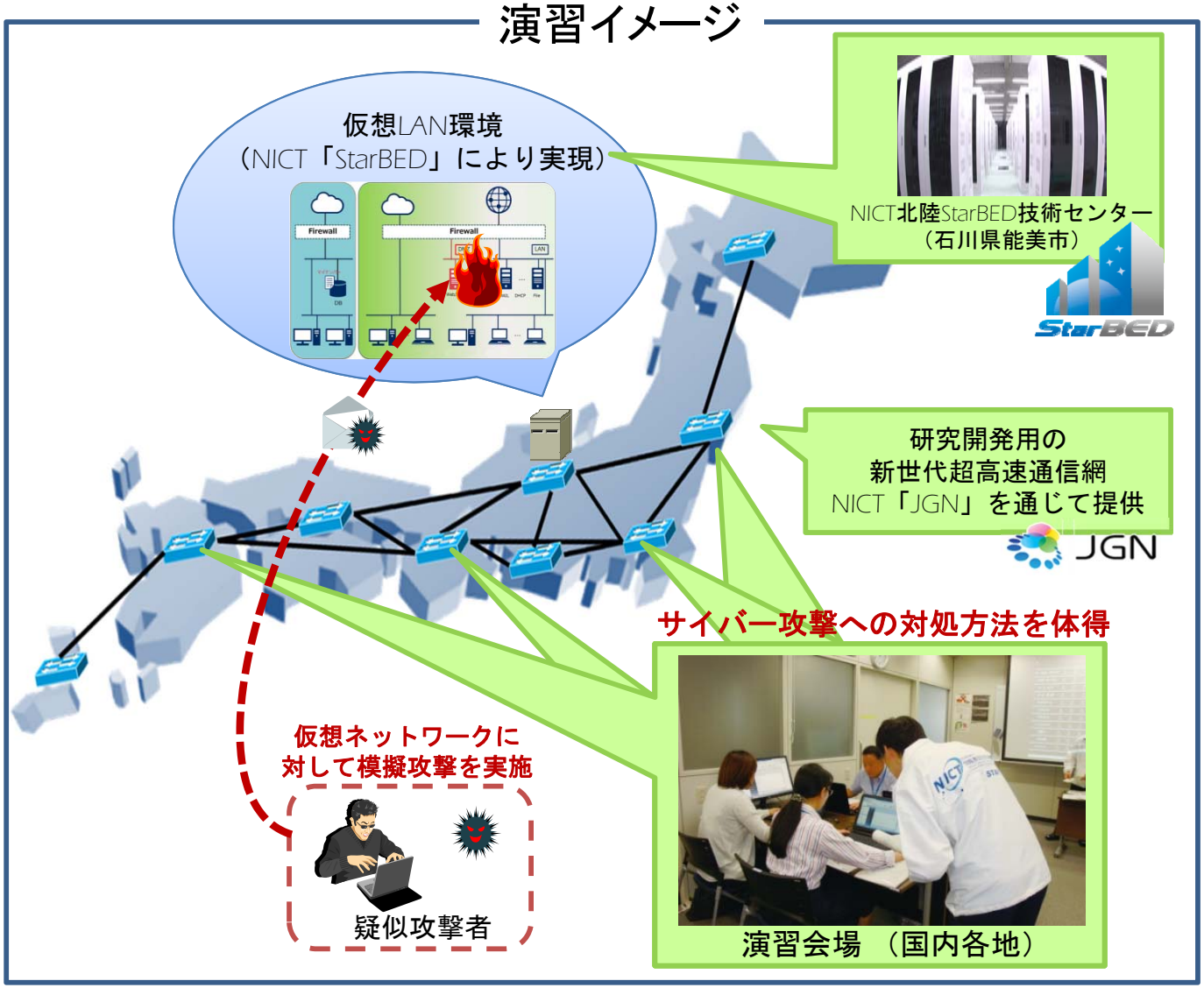
２－１－５．CYDER設問例

サイダー　サイバー　防御　反復演習

2-1-1.実践的サイバー防御演習（CYDER: CYber Defense Exercise with Recurrence）

政府のサイバーセキュリティ戦略及び情報通信研究機構法改正に基づき、国の行政機関、地方公共団体、重要インフラ事業者等を対象として、NICTが有するサイバーセキュリティの技術的知見及び大規模計算機環境を最大限に活かした実践的なサイバー防御演習を開発・実施

演習イメージ



演習の概要

- ✓ 受講者は組織の情報システム担当職員として演習に参加し、組織の LAN 環境を模擬した環境で標的型攻撃によるインシデントの検知から対応、報告まで一連の流れを体験しながら学ぶ。

演習の特徴

- ✓ NICT 北陸 StarBED 技術センターに設置された大規模高性能サーバ群を活用し、仮想ネットワーク環境として演習環境を構築
- ✓ NICT における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、最新の演習シナリオを用意

■対象組織
サイバーセキュリティ基本法に規定される、
・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

■開催規模（平成29年度／予定）
全国47都道府県で合計100回3000人実施予定

2-1-2.CYDERの沿革・実績

2013～2015年度
・総務省の実証実験としてスタート
・NICTは大規模演習環境を提供

2015年9月
・**サイバーセキュリティ戦略**(閣議決定)

政府機関、重要インフラ等の実践的な演習・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となった**。

2016年4月
・**改正NICT法成立** (5月施行)

CYDERの事業主体をNICTに変更することにより、安定的・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った。

〇受講資格

・国の行政機関
・独立行政法人
・特殊法人・認可法人
（サイバーセキュリティ戦略本部が指定する法人に限る）
・地方公共団体
・重要社会基盤事業者

〇実績（参考）総務省実施

2013年度　33組織292名
2014年度　61組織215名
2015年度　78組織208名

全地方公共団体の約30%が受講！

〇2016年度実施状況

〇受講枠（当初予定）

390組織1,170名
※1組織1～4名程度

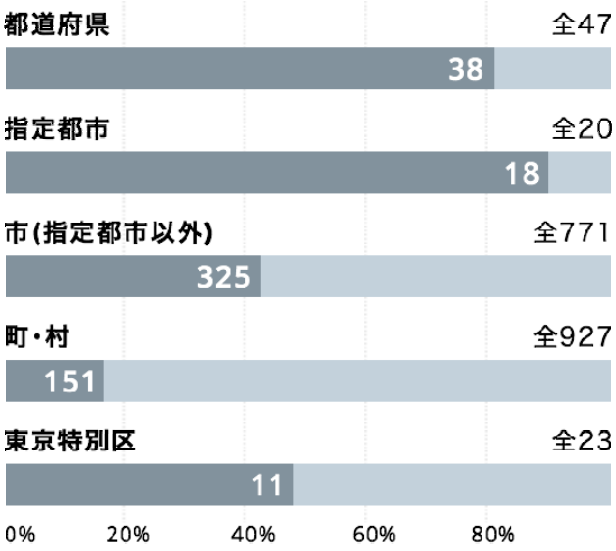
〇申込数

1015組織1,993名

〇受講数

765組織1,539名
うち、国の行政機関等：205組織420人
地方公共団体：560組織1,119人

H28年度演習受講組織数・受講者数
（地方公共団体）



2-1-3.平成29年度CYDER年間開催日程(予定)

(Aコース)59回

			回数				
1	北海道	北海道	2	札幌7/19	帯広8/31		
2	東北	青森県(青森)	1	7/25			
3	東北	岩手県(盛岡)	1	7/27			
4	東北	宮城県(仙台)	2	6/26	10/10		
5	東北	秋田県(秋田)	1	8/1			
6	東北	山形県(山形)	1	8/23			
7	東北	福島県(郡山)	2	8/25	9/28		
8	関東	茨城県(水戸)	1	7/25			
9	関東	栃木県(宇都宮)	1	8/29			
10	関東	群馬県(前橋)	1	7/12			
11	関東	埼玉県(さいたま)	1	7/10			
12	関東	千葉県(千葉)	2	9/11	10/26		
13	関東	東京都(東京)	4	6/20	6/22	8/4	9/15
14	関東	神奈川県(横浜)	1	9/13			
15	関東	山梨県(甲府)	1	9/5			
16	信越	新潟県(新潟)	1	6/28			
17	信越	長野県(長野)	1	7/14			
18	北陸	富山県(富山)	1	6/30			
19	北陸	石川県(金沢)	1	10/5			
20	北陸	福井県(福井)	1	10/3			
21	東海	岐阜県(岐阜)	1	7/5			
22	東海	静岡県(静岡)	1	7/7			
23	東海	愛知県(名古屋)	3	6/26	8/21	10/30	
24	東海	三重県(津)	1	7/14			
25	近畿	滋賀県(大津)	1	6/30			
26	近畿	京都府(京都)	1	7/4			
27	近畿	大阪府(大阪)	3	6/28	8/23	11/1	
28	近畿	兵庫県(神戸)	1	7/6			
29	近畿	奈良県(奈良)	1	7/10			
30	近畿	和歌山県(和歌山)	1	7/12			
31	中国	鳥取県(鳥取)	1	10/17			
32	中国	島根県(松江)	1	10/19			
33	中国	岡山県(岡山)	1	8/25			
34	中国	広島県(広島)	1	8/28			
35	中国	山口県(山口)	1	8/30			
36	四国	徳島県(徳島)	1	8/3			
37	四国	香川県(高松)	1	8/1			
38	四国	愛媛県(松山)	1	11/7			
39	四国	高知県(高知)	1	7/28			
40	九州	福岡県(福岡)	2	9/1	9/13		
41	九州	佐賀県(佐賀)	1	9/5			
42	九州	長崎県(長崎)	1	9/7			
43	九州	熊本県(熊本)	1	10/24			
44	九州	大分県(大分)	1	9/15			
45	九州	宮崎県(宮崎)	1	10/11			
46	九州	鹿児島県(鹿児島)	1	9/20			
47	沖縄	沖縄県(宜野湾)	1	7/19			

(B-1コース)21回

		回数				
1	北海道(札幌)	1	10/24			
2	東北(仙台)	2	9/29	10/18※		
3	関東(東京)	4	9/12	9/19	10/4	11/7
4	信越(新潟)	1	10/6			
5	東海(名古屋)	3	9/22	9/28	10/31	
6	近畿(大阪)	3	9/7	9/26	11/2	
7	北陸(金沢)	1	10/12			
8	中国(広島)	1	10/20			
9	四国(松山)	1	11/9			
10	九州	3	福岡9/22	福岡10/13	熊本10/25	
11	沖縄(宜野湾)	1	10/31			

※10/18午後開始・10/19午前終了

(B-2コース)20回

		回数	
1	東京	1	12/12
2	東京	1	12/13
3	東京	1	12/14
4	東京	1	12/15
5	東京	1	12/18
6	東京	1	12/19
7	東京	1	12/20
8	東京	1	12/21
9	東京	1	12/22
10	東京	1	1/9
11	東京	1	1/10
12	東京	1	1/11
13	東京	1	1/12
14	東京	1	1/15
15	東京	1	1/16
16	東京	1	1/17
17	東京	1	1/18
18	東京	1	1/19
19	東京	1	1/22
20	東京	1	1/23

Aコース:初心者向け(平成29年度新設コース)
Bコース:コンピュータ及びネットワーク並びにサイバーセキュリティに関する
基礎知識を既にお持ちの方向け
B-1コース:地方公共団体向け
B-2コース:国の行政機関、独立行政法人、指定法人、
重要社会基盤事業者向け

2-1-4.平成29年度CYDER演習内容

カリキュラム（Aコース・Bコース）

Aコース（59回）：初心者向け（平成29年度新設コース）
Bコース（41回）：コンピューター及びネットワーク並びにサイバーセキュリティに関する基礎知識を既に持つ者向け

事前オンライン学習（講義演習パート）

最近の標的型攻撃の傾向や対策を理解し、インシデントハンドリングの心得について学ぶ。

実　習（実機演習パート）

チームに分かれ、インシデントハンドリングを一通り体験し、報告書を作成。

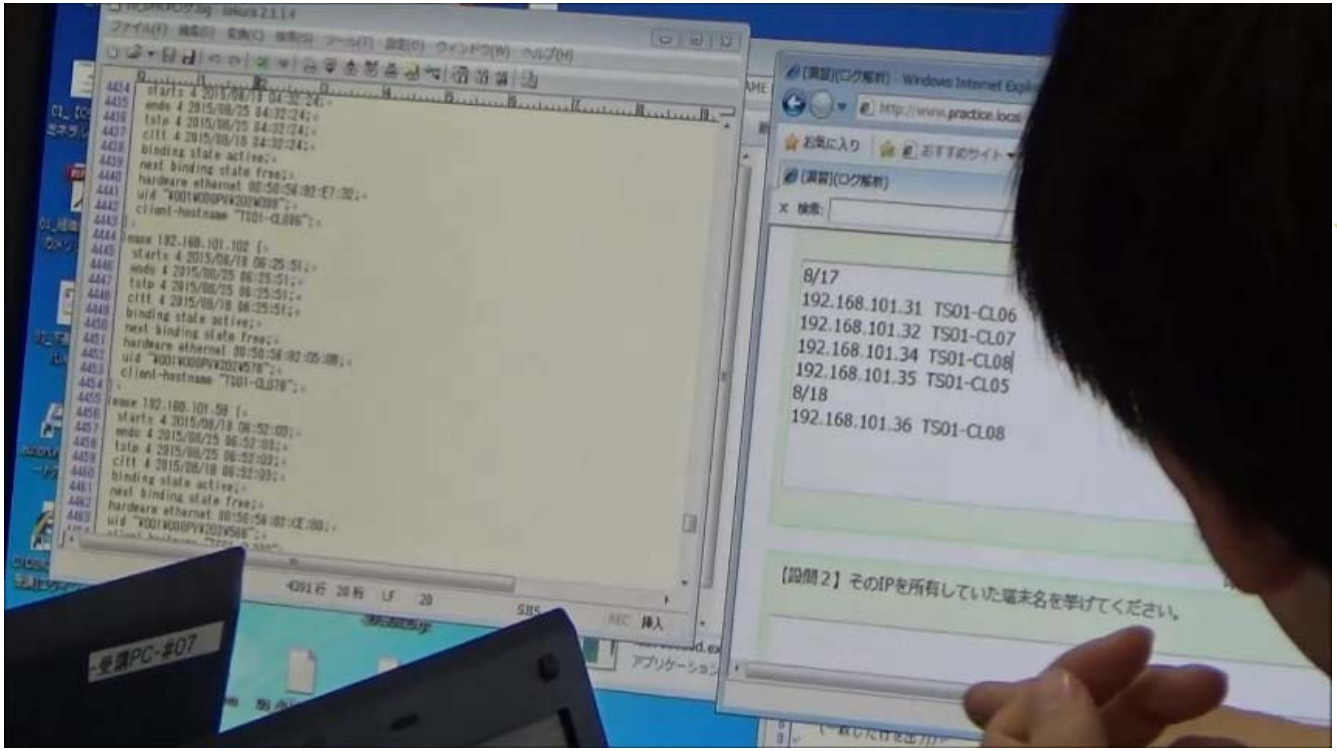
グループワーク

実習を通して気づいたポリシーや運用面の課題を明確にし、対策を検討するディスカッションを行う。

体験のみで終わらない本格的なトレーニングを受講することが可能！

2-1-5.CYDER設問例(イメージ)

SOC業務委託業者から、海外にあるC&Cサーバーとの通信を検知したとの連絡を受けました。委託業者より提供された以下のC&Cサーバー情報を基に各種ログを解析し、このサーバーに通信を行った端末を特定してください。
【C&Cサーバー情報】 IPアドレス：x.x.x.x .....



C&Cサーバーと通信した端末(IPアドレス)を各種ログから特定しています。

2-2.2020年東京オリンピック・パラリンピック開催に向けたサイバー演習による人材の育成（サイバー・コロッセオ）

概要

2020年東京オリンピック・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の育成を行う。また、関係組織が一体となった演習を実施することで個々の組織の強化だけでなく、組織間の連携も強化する。

イメージ図

攻防戦によるサイバー演習

具体的内容

- 大規模クラウド環境を用いて、公式サイト、大会運営システムや、社会インフラの情報システム等を模擬したシステムを構築。
- 当該システムにより、大会開催時に想定されるサイバー攻撃を再現し、大会組織委員会のセキュリティ担当者を中心に、攻撃・防御手法の検証及び訓練を行う。

大規模な演習を実施し、2020東京大会のサイバーセキュリティを確保

２－３．若手セキュリティエンジニア育成プログラム（SecHack365）

２－３－１．若手セキュリティエンジニア育成プログラム“SecHack365”について

２－３－２．　具体的な実施内容

２－３－３．年間スケジュール

2-3-1.若手セキュリティエンジニア育成プログラム“SecHack365”について

■ 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。

事業の特徴

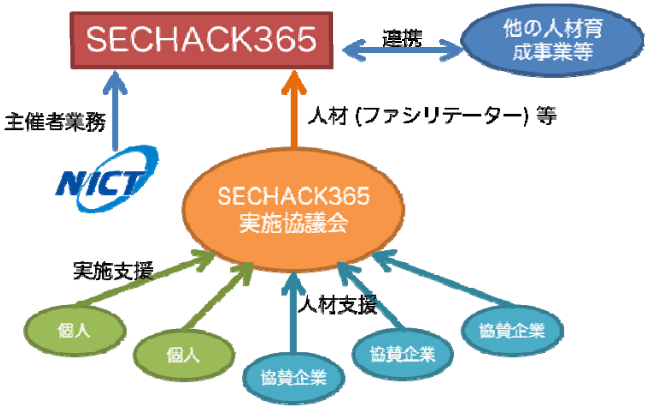
- **NICT の強みを活かした育成事業**
  - ✓ 学生、若手社会人を対象とした早期人材育成
  - ✓ アイディアソン、ハッカソン、遠隔開発、演習の組み合わせによる総合的能力開発
  - ✓ １年という長期間の取り組みにより教育効果を増大
  - ✓ NICT が有する最先端の研究開発のノウハウ、研究資産(攻撃データ等) の利活用

期待される成果

- **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
  - ✓ 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

実施体制

- **NICT と実施協議会との共催**
  - ✓ 協賛企業、個人による実施協議会に人材、ノウハウを集約し、迅速な事業運営を図る



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）
	H29.5.9受講者決定時点

SecHack365

2-3-2.具体的な実施内容

事業内容

✓ 定期的にアイディアソン、ハッカソン、コンテスト演習を実施するほか、NICT の遠隔開発環境を活用し定期イベントのない期間も定常的に開発の機会を提供し、ハイレベルな研究者・実務者を育成する。

アイディアソン・ハッカソン

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開発を行う (計 6 回程度)
- ✓ 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

アイディアソン・ハッカソンイメージ

遠隔開発実習

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

※*遠隔開発環境 （NONSTOP）*

遠隔からNICTのクラウド環境を利用し、サイバー攻撃等の実データ・解析ツール、チャット機能等を使いながら、技術開発ができる。

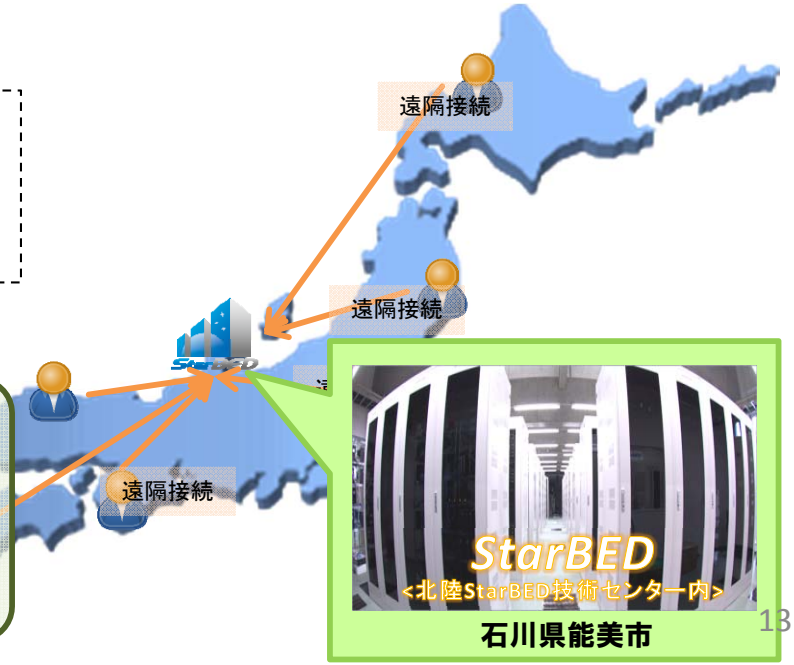
ハッカソンのテーマ例

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

コンテスト演習

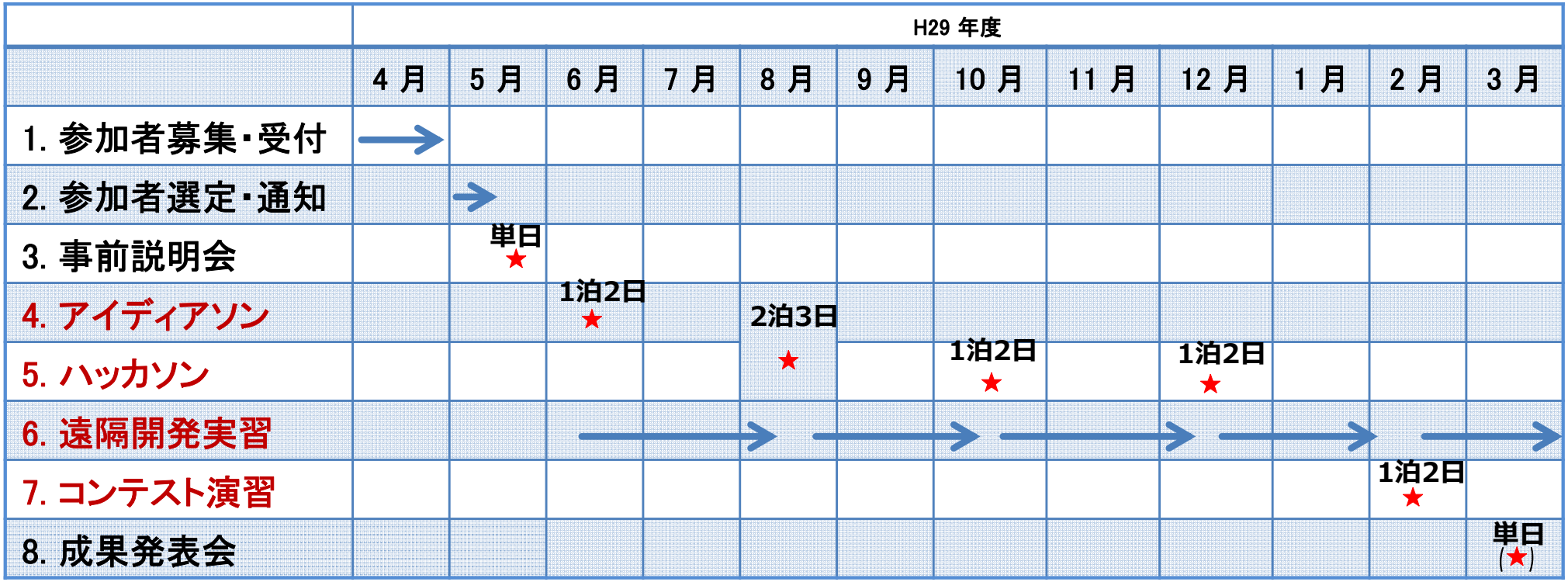
最終総合評価

- ✓ コンテスト形式による受講者の総合評価
- ✓ 模擬環境上で各自が作成したツールを活用しながら与えられた課題に挑戦し、成績を競う
- ✓ NICT 小金井本部にて実施



2-3-3.年間スケジュール

年間スケジュール



イベントの開催日程、場所

※優秀者（若干名）に対し、海外派遣も実施予定 (検討中)

開催回	日程	場所	企画内容
5 月回	5 月 19 日(金)～20 日(土)	NICT 小金井	NICT 見学 (19日)、説明会 (20日)
6 月回	6月10日(土)～11日(日)	東京	アイディアソン
8 月回	8月23日(水)～25日(金)	福岡	ハッカソン
10 月回	10月14日(土)～15日(日)	北海道	ハッカソン
12 月回	12月23日(土)～24日(日)	大阪	ハッカソン
2 月回	2月24日(土)～25日(日)	沖縄	コンテスト演習
3 月回	3月24日(土)	NICT 小金井	最終報告会

３．ナショナルサイバートレーニングセンターの今後の方向性

３－１．CYDERの今後の方向性

３－２．SecHack365の今後の方向性

3-1.CYDER の今後の方向性

演習「規模」の拡大（実機オンライン演習システムの研究開発）

現況

毎年、受講枠を大きく上回る受講希望があり、人数制限を実施

参考：
H28年度　受講枠 390組織1170人　：1015組織1993人から申込み
H29年度　受講枠1000組織3000人　：地方公共団体だけで900組織以上、2700人以上の受講希望（事前のニーズ調査）

今後の対策

【実機演習パート（実習）】のオンライン化を検討。
＊既に講義演習パートはオンライン化済（H29年度～）

期待できる成果としては‥

- 受講者数の拡大
- 低コストで演習受講が可能
- 時間＆場所を問わずStarBEDにアクセス可能

演習「内容」の更なる充実

(1) 演習シナリオの不断の見直し

★世界的規模で重要かつ新手のインシデントが発生

★引き続きNICTERで観測した直近の攻撃データ等をもとに徹底的に分析し、演習シナリオを不断に見直し＆更新

(2) 演習シナリオの更新作業の効率化

最新シナリオへの更新をより効率的かつ迅速に行うため、システムの研究開発を進める。

期待できる成果としては‥

- 最新シナリオへの更新をより効率的かつ迅速に行うことが可能
- 受講者のスキルレベルや産業分野に合わせたシナリオ最適化

3-2.SecHack365の今後の方向性

SecHack365は、H29年4月から開始したばかりの新規事業であり、初年度の運用をしっかり見極める必要がある。
なお、少なくとも次の２点については、引き続き意欲的に取り組みたい。

教育機関、産業界との連携推進

具体策

★高等専門学校、大学等が実施している若手向けの育成プログラムとの連携推進

★有志のビジネスパーソンによる実施協議会への参画等の促進

⇒若手人材がビジネス現場と早い段階から交流することが可能になる！

⇒新たなアイデアのヒントを得ることでき、且つ幅広い人脈を形成することが可能になる！

SecHack365コミュニティの形成

具体策

★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となる

⇒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が可能となる！

⇒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となる！