［セキュリティ人材育成の現状と実践］

②社会におけるセキュリティ人材育成事例（1）―NICTにおけるセキュリティ人材育成事業―

応般

安田真悟 | 国立研究開発法人情報通信研究機構　サイバーセキュリティ研究所　サイバーセキュリティ研究室／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

ナショナルサイバートレーニングセンターの設立

セキュリティ人材の育成が喫緊の課題となっている現在，国立研究開発法人 情報通信研究機構（以下，NICT）は，情報通信分野を専門とする我が国唯一の公的研究機関として，NICTの技術的知見，研究成果および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「ナショナルサイバートレーニングセンター」を2017年4月1日に設置した．当センターは，現在，「セキュリティオペレータ（実践的運用者）」と「セキュリティイノベータ（革新的研究・開発者）」の2つのサイバーセキュリティにかかわる人材分野を主たる育成領域として，図-1に示す以下の3つの人材育成事業を行っている．

- セキュリティオペレータ領域
  - CYDER
  - サイバーコロッセオ
- セキュリティイノベータ領域
  - SecHack365

セキュリティオペレータ領域の2事業は組織内の情報セキュリティ問題を専門に扱うCSIRT（Computer Security Incident Response Team）の要員育成を軸にCYDERでは初級～中級まで，サイバーコロッセオでは初級～準上級までの人材育成プログラムを実施している．

セキュリティイノベータ領域では，将来の日本を支えるサイバーセキュリティ研究者・起業家の創出を主軸に，25歳以下向けの人材育成プログラムを実施している．

本稿では，これら3事業の取組みを紹介するとともに，これらの事業を通して得られた知見と現在のサイバーセキュリティ，人材育成における課題を述べる．

CYDER

ナショナルサイバートレーニングセンターの中核事業である実践的サイバー防御演習「CYDER（サイダー；CYber Defense Exercise with Recurrence）」（図-2）は政府のサイバーセキュリティ戦略等に基づき，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，重要社会基盤事業者等を対象として2016年度より実施している人材育成事業である．2017年度からは年間約100回の演習を全国で実施するまでに規模

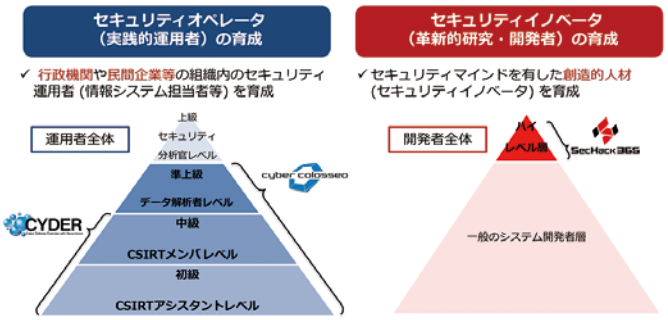

図-1　ナショナルサイバートレーニングセンター事業領域

を拡大し，2018 年度までの 3 年間で 246 回の演習を実施し，のべ 7,174 人の受講者を輩出している．

本事業の最大の特徴は行政機関等の情報セキュリティ人材の質，高スキル人材の大都市地域への偏在を是正するため，初級である A コースは全国 47 都道府県すべてで，中級向けの B コースも全国 12 の主要都市で開催し，地方の市町村レベルの地方公共団体職員等に対しても受講機会を提供していることが挙げられる．ICT の利活用の促進，自治体クラウドの導入やマイナンバー制度導入など，地方自治体の情報システムを取り巻く環境が大きく変化する中で，地方公共団体，重要社会基盤事業者にはその業務の実施においてサイバーセキュリティに対する相応の能力が求められている．しかしながら地方で開催されるセキュリティに関する講習会等は少なく，また都市部で開かれる講習会等に職員を送り込むことは予算や人員的負担が大きい．また，都市部との待遇の格差のため高度な人材の獲得が困難，といった課題を抱えている．しかし，サイバー空間では都市部と地方とに関係なく攻撃に晒されるため，特に地方におけるセキュリティ人材育成は喫緊の課題である．

CYDER を実施するにあたり，事前に行った全国自治体への CYDER 受講の希望を問うニーズ調査では，回答があった自治体の中で参加を希望する自治体は 86％であった．参加しないと回答した自治体にその理由を尋ねる設問では，地元のイベントとの日程の重複等，開催日に関する問題のほかに，移動宿泊費の不足を挙げる自治体もあった．また，開催地の希望に関する設問においては，県域が広い自治体では主に県庁所在地である県内開催地が遠いため，近隣での開催を希望する回答があるなど，地方自治体向けの演習の課題が浮き彫りとなった．そのため，2019 年度の CYDER では県域が広い自治体では複数の開催地を設定する等，受講機会拡大の施策を進めている．

CYDER の演習カリキュラムは初級向け A コースと中級向けに B-1，B-2 コースがある．どのコースも図 -3 に示す 1 時間程度のオンライン予習と 1 日の集合演習で構成されている．集合演習では実機を用いて，架空の組織で発生したセキュリティ事故のインシデントレスポンス（原因の特定，除去，復旧，必要な外部組織への連絡等セキュリティ事故全般への取組み）を行う演習を実施し，最終的にインシデントレスポンスの報告書を作成する．

実機演習ではコース別に最適化されたリアルな仮想環境を用意している．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，コース別に表 -1，表 -2 に示すような最新のシナリオを毎年提供している．毎年シナリオを更新することで，繰り返し受講を促し，最新かつさまざまな攻撃への対処法を学ぶことができる演習となっている（図 -4）．

サイバーコロッセオ

サイバーコロッセオは 2020 年東京オリンピック・

図 -2　CYDER 演習風景

図 -3　CYDER 演習カリキュラム

パラリンピック競技大会の円滑な実施を支援するため，東京オリンピック・パラリンピック競技大会組織委員会および業務受託ベンダ等の関連組織の職員を対象としたセキュリティ人材育成事業である．サイバーコロッセオは「コロッセオ演習」と「コロッセオカレッジ」の2種類のカリキュラムで構成されている．「コロッセオ演習」は，CYDERで培った知見に基づく初級・中級の演習に加えて，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準上級コースを開講している（図-5）．2017年度より開始された本事業は，段階的に規模を拡大し，2020年には3コース（初級・中級・準上級）で220人規模の人材育成を目標としている．「コロッセオ演習」のカリキュラムは表-3に示すように，レベルのほか受講者の職務領域を考慮して各レベル複数コースを編成しており，2019年度には初級2コース，中級2コース，準上級3コースの合計7コースを開講している．

「コロッセオカレッジ」は「コロッセオ演習」と密に連携し，コロッセオ演習を受講する上で必要な前提知識や周辺知識を習得し，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年度から新設された補助講義演習群であり，初級，中級，準上級のコロッセオ演習と連携し表-4に示す合計20科目のセキュリティ関連科目を開講している．

表-1　演習シナリオ例（2018年度Aコース）

Aコース	
侵入	USBメモリによる侵入
C&C通信	HTTP通信
横展開	OSの脆弱性を利用
漏洩	HTTP通信による持ち出し
攻撃シナリオ概要	OSの脆弱性を利用するマルウェアに感染したUSBメモリを取引業者から受領し，端末に挿入して感染．マルウェアがRATをダウンロード．RATにより内部感染．MS14-068の脆弱性を利用してドメイン管理者権限を取得され，ドメインユーザを作成，管理者権限を付与，ファイルサーバから端末の1台に機密情報がコピーされ，プロキシサーバを経由して外部へアップロード．
インシデントハンドリングの流れ	1. SOC委託業者がC&Cサーバとの通信を検知し，CSIRTに通知． 2. CSIRTが，C&Cサーバと通信していた全端末を特定． 3. その端末がマルウェアに感染し，RATをダウンロードしてほかの端末に感染拡大させていたことを特定． 4. 保全した感染端末の証拠から，感染源を特定． 5. 封じ込めとしてC&Cサーバ，RATダウンロードサイトへの通信遮断と注意喚起 6. ファイルサーバ上の機密情報が，ある職員端末経由で送信されていたことをCSIRTが特定． 7. 最新のマルウェア定義ファイルを全端末とサーバに適用，フルスキャンを実施して復旧．
ハンズオン	プロキシログ調査 ディスクイメージ調査 マルウェア解析

表-2　演習シナリオ例（2018年度Bコース）

Bコース（B-1コースの例）	
侵入	アプリ配布サイト改ざん
C&C通信	DNS通信
横展開	SMBサーバ脆弱性攻撃
漏洩	DNS通信による持ち出し
攻撃シナリオ概要	改ざんされたアプリケーションをダウンロードした端末Xが，マルウェアに感染．DNSトンネリングでC&Cサーバと通信．脆弱性（MS17-010）を利用，内部感染．保存されていたシステム管理者である職員のDMZサーバアカウントを取得．DMZの外部メールサーバにsshで侵入，外部メールサーバから組織外へフィッシングメールを送信．端末Yに保管されている機微情報をDNS通信でC&Cサーバに送信．
インシデントハンドリングの流れ	1. JPCERT/CCから，フィッシングメールが外部に送信されたことを確認した旨の通知 2. メールヘッダ・SPFレコードの調査により，端末Wのメールアドレスからフィッシングメールが送信されていたことが判明． 3. 端末Yが外部メールサーバに対して不審なアクセスを行っていたため，端末Yをネットワークから隔離し，アカウントYを停止． 4. 端末Y，外部メールサーバのフォレンジック調査をBセキュアに依頼． 5. 端末Xからも DNSによる不正な通信が発生していたことが判明，フォレンジックを依頼． 6. 端末Xのフォレンジック調査から，侵入経路・横展開に使われた脆弱性が判明． 7. メールサーバのリストア，最新のマルウェア定義ファイルを全端末・サーバに適用．メールサーバのリストアを行って復旧．
ハンズオン	メールヘッダ確認 DNS名前解決ログ調査 HDD，レジストリ等調査

図-4　CYDER演習の流れ

コロッセオカレッジは選択受講制を採用しており，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する．自身が受講予定のコロッセオ演習に対応した講義を事前に受けることを推奨しているものの，最新セキュリティトレンドや個人情報保護関係法令，EU 一般データ保護規則（GDPR）など，すべてのレベルの受講者を対象とした科目も受講可能である．また 2019 年度から初級～準上級のコロッセオ演習，コロッセオカレッジ全 20 科目を一部を除き年間 3 回ずつ開講し，多忙な組織委員会職員等への受講機会の拡大を行っている．

SecHack365

ナショナルサイバートレーニングセンターでは多様化・悪質化するサイバー攻撃に対抗するため，新たなソフトウェア等を自ら「研究・開発」できる人材の育成を目的として，25 歳以下の若手セキュリティイノベータ育成プログラム SecHack365 を 2017 年度から実施している（図 -6）．新エネルギー・産業技術総合開発機構（NEDO）の「平成 29 年度日系企業のモノと サービス・ソフトウェアの国際競争ポジションに関する情報収集」によると，日系企業が販売するウィルス対策ソフトの BtoC における世界シェアは 14.7%，ゲートウェイセキュリティ（FW・UTM）では 1% であり，我が国のサイバーセキュリティ産業の，世界のセキュリティ市場における存在感は決して大きくない．サイバー攻撃が多様化・悪質化する現在において，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ユーザとして「利用」するだけでなく，新たなソフトウェア等を自ら「研究・開発」していくことができる人材を育成していく必要がある．

図 -5　サイバーコロッセオ演習風景

表 -3　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	初級 A 初級 B	業務領域別で A/B のシナリオ作成
中級 CSIRT メンバ	中級 A 中級 B	繰り返し受講を想定して A/B シナリオ作成
準上級 データ解析者	準上級 A 準上級 B	A/B は攻撃主体の攻防戦
	準上級 C	防御主体の攻防戦

表 -4　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

図 -6　SecHack365 集合回風景

SecHack365 は年間 40 名程度の受講者（トレーニー）を選抜し，図 -7 に示すように，年間 6 回の全国各地で行われる合宿形式の集合回と，集合回の間のサポートをするオンラインサポート期間とで構成される．また，各分野のエキスパートに指導者（トレーナー）として参加していただき，1 年を通してトレーニーのものづくりを指導している．1 ～ 5 回目までの集合回ではアイデアソン，ハッカソン，倫理教育，企業見学，成果の途中発表などが行われる．そして，6 回目の集合回で成果の審査（図 -8）を行い，3 月に成果発表会（図 -9）を行う．創りたいものは基本的にトレーニーが自ら考え提案することを前提としているため，トレーニーの技術力や社会課題へのアプローチの違いから，進捗や進め方に違いがある．そのため，募集時からアプローチ別にコースを分けて募集を行っている．2018 年度からは以下の 5 つのコースを用意し，トレーニーのものづくりに対するアプローチの違いをふまえた指導を行っている．

- 表現駆動コース
  - アイディアをかたちにする，その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るサービスづくりをすすめる
- 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
  - 付加学習により他技術や他分野を知ることで，作るもののアイディアの幅を広げる
- 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
  - 開発テーマや分野が定まっている受講生を受け入れて開発を進めるための指導を実施する
- 思索駆動コース
  - 思索を通じて問題を深掘りし，その解決を行うコース
  - 日常に遍在する違和感に立ち向かう人材を育成する

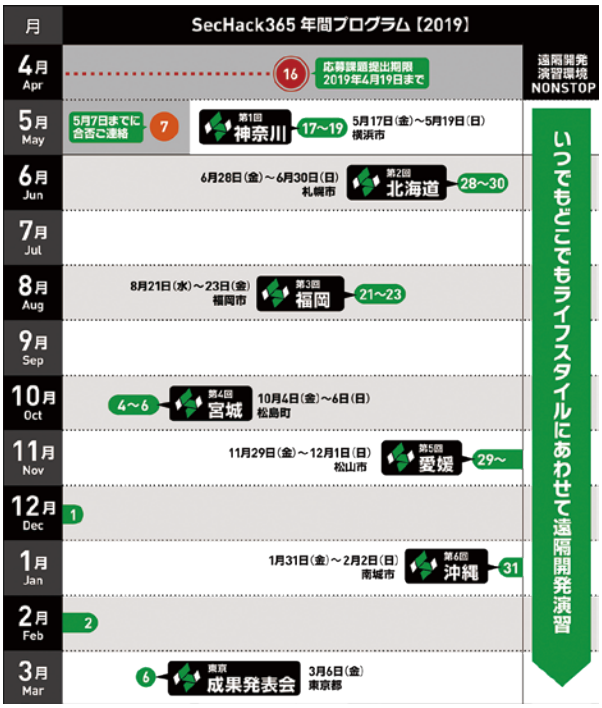

図 -7　SecHack365 2019 年度スケジュール


図 -8　SecHack365 沖縄回（成果審査会）


図 -9　成果発表会

- 研究駆動コース
  - 研究的プロセスに基づいたアイディア，仮説立案と検証評価を重視したコース
  - 研究者的なスキルを磨いて，将来の研究者になり得る人材を育成する

2年間を終えて，全64プロジェクトが成果発表を行い，12の優秀プロジェクトが選定された．優秀プロジェクトとして選出されたプロジェクトはプライバシに配慮したTwitterクライアントから，仮想空間でサイバー攻防を体験できるゲーム，CanSatと呼ばれる衛星技術教育を目的とした小型の模擬人工衛星を用いた競技会向けのリファレンスモデルの設計と知見の公開共有プロジェクトなど多岐にわたる．このような領域の広さは，SecHack365の特徴である．セキュリティは対策技術だけでなく，システムやソフトウェアの設計段階，開発の初期段階からセキュリティを考慮する「セキュリティバイデザイン」が重要と考え，イノベーションの領域の制約は少なくしているからである．同時に，多様な領域に興味を持つトレーニー同士の相互刺激がさらなるイノベーションの源泉となり活発な活動を支えている．また，NICTでは修了後の活動の支援や，その後のSecHack365のイベントへの招待など，SecHack365の修了生コミュニティの醸成にも努めている．

人材育成の課題

本稿では，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3事業を紹介した．本章ではセキュリティ人材育成における，現状と今後の課題を述べる．

セキュリティ人材の不足という喫緊の課題に対応するためCYDERでは年間3,000人規模の育成を行っている．しかし，セキュリティ人材育成においては講師の不足も課題となっている．特に地方においては，サイバーセキュリティに関する講座や勉強会等の学習機会が限られており，社会的な需要に対して十分な機会を提供できていない．サイバーセキュリティ人材を全国的に確保するためには，CSIRT要員の育成に加えて，CSIRT要員を指導できる講師を増やすとともに，民間の人材育成産業の成長を促進することも必要といえる．

また，育成対象の若手人材へのシフトも重要である．セキュリティはあらゆるICTにかかわり考慮されるべき必須項目であり，前述したセキュリティバイデザインの概念で提唱されているように，一般のシステム開発や創造的サービスの検討時にも初期の段階から考慮する必要がある．このような初期の段階からセキュリティの考慮を継続して着実に行うためには将来を担う若手人材の教育が重要である．若手人材育成の領域に向けてはSecHack365で人材育成を行っているが創造的人材を主眼としているため，人材育成の規模としては限定的となっている．

他方，セキュリティはICTを利用する側にも基本的な理解が必要であり，育成すべき人材はエンジニアにとどまらず，利用者となる事務職なども含まれる．人材不足のニーズにより官民を挙げてセキュリティ人材の育成に取り組んでいるが，現役世代に対する教育は一種の対症療法であり，本来，情報分野やイノベーションを担う創造的人材は言うに及ばず，事務職総合職を担う学生に向けても基本的なセキュリティ教育が必要である．しかし，この領域の人材育成・教育対象者はエンジニアよりも多く，全国的規模で教育を行うためには高校や大学などの既存高等教育の各科目と同等の教育者の人数を必要とする．中長期的には高校や大学などでの基本教育の一環としてのセキュリティ教育により，広範な領域に従事する人材の情報セキュリティリテラシーを向上することが必要であり，その指導を担う教育人材の育成も今後の課題であるといえる．

(2019年7月17日受付)

安田真悟　s-yasuda@nict.go.jp
博士（情報科学）．北陸先端科学技術大学院大学産学官連携研究員を経て現職情報通信研究機構入構．サイバーセキュリティ研究室，ナショナルサイバートレーニング研究室兼務．標的型攻撃等の観測・解析環境の構築技術などの研究に従事．近年は人材育成への応用に取り組む．