セキュリティオペレーション人材の現状と育成に向けた取組み

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（えとう）　将史（まさし）

1. セキュリティ人材不足に関する状況

サイバー攻撃の巧妙化、深刻化を受けて、サイバー攻撃対策の重要性が増す一方で、その対策を担うセキュリティ人材の不足が社会的な課題となっている。日本国内では、2014年のIPAの報告[1]において14万人あまりの人材教育の必要性が明らかにされたのをはじめとして、内閣サイバーセキュリティセンター（NISC）は、2015年のサイバーセキュリティ戦略[2]においてセキュリティ人材が「質的にも量的にも圧倒的に不足している」と指摘した。また、経済産業省による2016年の報告[3]は、セキュリティ人材の不足が2020年の時点で19.3万人に拡大すると推計している。

2. NICTにおける人材育成事業

このような深刻なセキュリティ人材の不足に対処するため、NICTナショナルサイバートレーニングセンターでは図1に示すとおり、実践的サイバー防御演習「CYDER（サイダー）」、東京2020オリンピック・パラリンピック競技大会（以下「東京2020大会」）開催に向けたサイバー演習「サイバーコロッセオ（CYBER COLOSSEO）」、そしてセキュリティイノベーター育成事業「SecHack365（セックハックサンロクゴ）」の三事業を推進している。

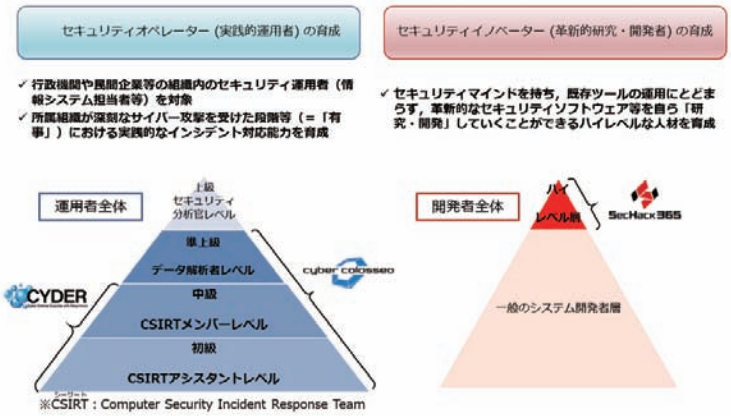
3. NICTにおける取組み① 実践的サイバー防御演習「CYDER」

実践的サイバー防御演習CYDERは、サイバー攻撃を受けた際の一連の対処行動を身につけるための、公的機関の職員を対象とした演習プログラムである。対象組織は2017年度現在、国の行政機関、地方公共団体、独立行政法人・指定法人及び重要社会基盤事業者となっている。これらの組織において、ITベンダ任せではなく、日常のシステム運用等を考慮しながら、事業継続を脅かす攻撃に対処することができる「総合力の高い情報システム管理者」を養成することがCYDERの目的である。

CYDERの最大の特徴は、NICTが長年にわたるサイバーセキュリティ研究において蓄積した知見や攻撃データに基づき、サイバー攻撃に係る我が国固有の傾向等を徹底的に分析し、現実のサイバー攻撃事例を再現した最新の演習シナリオを用意している点である。CYDERは図2のとおり事前のオンライン学習（講義演習：1時間程度）と集合演習（実機演習＋グループワーク：1日間）によって構成されている。はじめに、受講者は実習受講前にオンライン学習を受講し、ここでサイバーセキュリティに関する基礎や演習に必要な知識を学ぶ。

CYDERのオンライン事前学習はNICT北陸StarBED技術

■図2. CYDER演習の構成



■図1. NICT ナショナルサイバートレーニングセンターにおける三事業

センター内のLearning Management System（LMS）上に構築され、全国どこからでもWebブラウザを利用してインターネット経由でアクセス可能となっている。日常業務で忙しい受講者の負担を少なくするため、講義資料はインシデントハンドリングに必要な最低限の予備知識等をコンパクトにまとめ、60～90分程度で完了できる程度の分量にしている。さらに、業務の合間を使って飽きずに少しずつでも受講できるように、細かい章立て、項目立てにする、イラスト等を多用する、1項目当たりの受講目安を3～5分程度にするなどの工夫を行っている。

そしてCYDERの中心となる集合演習では、受講者が3～4人で1グループとなり、シナリオに沿ってインシデントハンドリングの手順（「検知・連絡受付」から「封じ込め」、「報告書作成」に至る一連の作業）を実際の機器やソフトウェアの操作を行いながら実践的に体験する。

ここではマルウェアに感染し不正な通信を行っている端末をProxyサーバ等のログから特定するといった、実際の現場で役立つ内容を数多く盛り込んでいる。このような演習シナリオには、NICTが持つサイバーセキュリティに関する最新かつ高度な知見を取り入れ、毎年新たなシナリオを作成している。例えば、今年度のBコースのシナリオは、今年世間を賑わせたWannaCryの事案やApache Struts2でも利用された、アプリケーションの脆弱性をねらう攻撃手法を想定した内容にしている。また、演習環境はLMSと同様にStarBED内に構築されており、グループごとに、実際の組織ネットワークを模した構成となっている。

最後のグループワークでは、これらの対応を自身の組織、環境、セキュリティポリシー等に置き換えた場合にどのように対処するか、といった視点での議論を行う。ここでは各グループでリーダーと書記を決め、実習を通して気付いた運用面等の課題や対策についての検討や、他グループに向けた発表を行う。また、受講前後にチェックテストを行うことで、受講によりどの程度の知識が身についたのかを確認する。

このようにCYDERは演習全体を通して得られた実践的な経験や知識を自組織に持ち帰り、それらを実際の現場で活用することに重点を置いた内容となっている。また、受講生のスキルレベルや進捗状況に応じたサポート体制も整っているため、セキュリティ初心者でも受講が可能となっている。

4. NICTにおける取組み②
東京2020オリンピック・パラリンピック競技大会開催に向けたサイバー演習「サイバーコロッセオ」

2020年に東京2020大会が開催予定であるが、このような全世界から注目される国際的かつ大規模なイベントは、攻撃者にとって格好のサイバー攻撃の対象となることが予想される。サイバー攻撃によるイベントの中止や関連業務の継続が妨げられることなく、適切に運営が維持されるよう、通常の業務に加え、サイバーセキュリティに関するノウハウの蓄積と人員強化が急務となっている。

当機構が実施するサイバーコロッセオは、東京2020大会の安定的な運営に向け、同大会関連組織のセキュリティ関係者を対象に行われるサイバー演習である。サイバーコロッセオでは、大会開催時を想定した模擬環境上で、攻撃・防御技術の双方に関する実践的な講義演習と攻防戦を主体とする実機演習を通じて、CYDER演習相当の技術レベルに加え、より一段階上のレベルの人材育成にも取り組む。

サイバーコロッセオの演習は東京2020大会の関係団体のうち、大会組織委員会の各部門とその担当システムベンダの職員を対象として実施される。また演習のレベルは**表**に示すとおり初級から準上級まで用意されており、受講者は自身の技術力に合わせて受講内容を選ぶことができる。

初級から準上級までの各コースは、技術実習を含む実践的なサイバーセキュリティ技術に関する座学と実機演習によって構成されている。特に準上級コースでは、Web、ネットワーク、フォレンジクス等、受講者の技術領域に特

■表．サイバーコロッセオのコース設定

	各コース受講時にあらかじめ必要な知識	受講対象者（育成したい人物像）
初級コース	・コンピュータ（特にWindows）に関する操作経験	・ユーザとしてのPC/NW 利用者で今後セキュリティ管理業務に従事する人
中級コース	・コンピュータとネットワーク（特にWindowsとTCP/IP）に関する基礎知識 ・サイバーセキュリティに関する基礎知識	・セキュリティ管理業務を主導する立場の人 ・インシデント対応にあたってユーザや内外関係部門との連絡調整役を担う人
準上級コース	・コンピュータとネットワーク（特にWindows, Linux/Unix、TCP/IP）に関する知識 ・サイバーセキュリティ（特にネットワークセキュリティ、バイナリ解析、フォレンジクス、ウェブセキュリティ、データベースセキュリティ、OSセキュリティ、ストラテジー／ガバナンスのいずれか）に関する知識	・高度なサイバー攻撃に対して自身の力で即時的に対処できる人 ・マルウェア検体や感染端末の詳細な解析技術を有する人

化した形での攻防戦を予定している。

以上のとおりサイバーコロッセオは、受講者の技術レベルや技術領域に応じた様々な教育コンテンツを用意し、攻防戦形式の演習を繰り返すことで受講者の能力向上を図る演習プログラムとなっている。本イベントは、今年度の開催を皮切りに2020年の大会本番に向けて継続的に実施され、関係組織のサイバー攻撃対応力の事前強化に取り組む予定である。

5. NICTにおける取組み③「SecHack365」

SecHack365は高度な技術力を持つ研究者や開発者育成により、日本のセキュリティ技術力、産業競争力向上を目指して、2017年度から開始されたプログラムである。

世界のサイバーセキュリティ市場における我が国のセキュリティ・ベンダの存在感は、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である。多様化・悪質化するサイバー攻撃に対抗し、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、単に既製品を「運用」するだけでなく、自ら新たな製品等を「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。

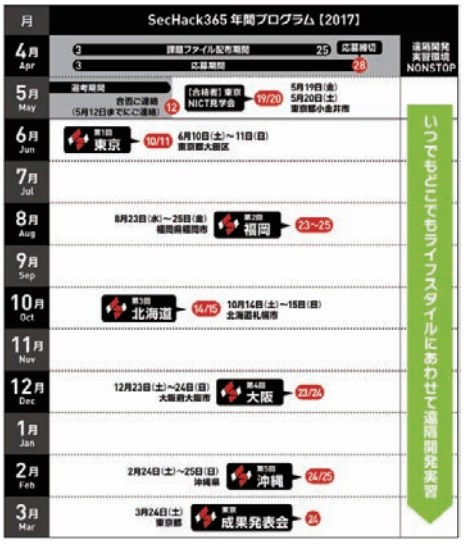
そのため、NICTナショナルサイバートレーニングセンターは、未来のサイバーセキュリティ研究者・起業家の創出に向けて、若手のICT人材を対象にセキュリティの技術研究・開発を本格的に指導する本プログラムを2017年度から開講している。

SecHack365では25歳以下の学生や若手社会人から公募を通じて40名程度の参加者（トレーニー）を選抜し、1年をかけてセキュリティ技術の研究開発を指導することで、ハイレベルな人材を養成する。年間プログラムの中では、**図3**で示すとおり、ハッカソン、遠隔研究・開発実習、コンテスト演習、座学講座、全国の一流研究者・技術者等との交流、先端企業の見学等のイベントを通じて、各参加者の志望に沿った能力開発を行う。

ハッカソン等の計7回の集合イベントと通年で実施される遠隔研究・開発実習を中核とする年間プログラム（**図4**）では、参加者は集合イベント以外の日も遠隔研究・開発実習により自分のライフスタイルに合わせてスキルを伸ばすことができる。

トレーニーは、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等を活用して、社会的に未解決の課題にチャレンジする研究・開発に取り組むことができる。

■図3. SecHack365のプログラムのイメージ図



■図4. SecHack365の年間スケジュール

より具体的には1年間のプログラムにおいて以下の取組みが行われる。

・ハッカソン／アイディアソン（イベント）

2か月に1回の頻度で計5回（1回あたり1泊2日または2泊3日）で実施するイベントではICT技術、セキュリティ分野で活躍する実施協議会委員のサポートのもと、仲間と一緒に最先端のセキュリティ関連技術の研究･開発を体験する。

・遠隔研究・開発実習

ハッカソン／アイディアソンのイベント以外の日は、遠隔研究・開発実習に取り組む。この実習では、トレーニーはNICTが用意したセキュリティ向け遠隔開発環境“NONSTOP”に自宅等からVPN経由で環境に接続し、トレーニー同士でコミュニケーションをしながらハッカソン研究・開発を継続することができる。

■写真1.　蒲田回アイディアソンの様子

■写真2.　福岡回ハッカソンの様子

・コンテスト演習

2月のイベントでは、それまでのハッカソンで得られた成果物や知見、取組みを評価するためのコンテストを行う。

・最先端の研究データの活用

ハッカソンや遠隔研究・開発実習で用いる遠隔開発環境“NONSTOP”では、NICTの長年にわたるサイバーセキュリティ研究によって得られた膨大なセキュリティ関連データを活用することができる。“NONSTOP”内に整備された様々な研究開発・解析用ツール類と、他では触れることのできない貴重なデータを用いて研究・開発に取り組む。

・全国の一流の研究者・技術者等との交流

国内各地で開催するイベントでは、様々な業界で活躍するプロフェッショナルの方々をスペシャルゲストとして招き、ハッカソンへの参加や講演をしていただいている。トレーニーたちは、専門家ならではの貴重な知見や技術からユニークな発想力を得ながら、優れた技術の研究・開発に取り組む。

・先端企業の見学等の社会体験

国内各地で開催するイベントでは、その地域において先端的な取組みを行っている企業の見学なども行う。ここでは、その地域ならではの体験を通じて発想力と感性を磨き、ハッカソンに活かすこととなる。

・修了証書の授与

1年間のプログラム修了後には、NICTが発行する修了証書が授与される。

以上のプログラムに対して、初年度となる2017年度は358名の応募があり、応募書類に基づいて、熱意と発想力といった観点で47名のトレーニーが選抜された。トレーニーが企業見学やゲストハッカーといった、環境や人々から刺激を受けて自由な発想やトレーニー同士の活発なコラボレーションを生み出だせるように、開催地を東京、福岡、北海道、大阪、沖縄と、様々な地域に設定し、イベントが実施された。

SecHack365の運営にあたっては、当機構及び外部のセキュリティ専門家の方々からなる「SecHack365実施協議会」を組織しており、実施協議会委員がトレーナーとしてトレーニーへの技術的なサポートをしている。

また昨今、セキュリティに関する知識はあるものの、倫理や法制度までは理解していない若年層によるサイバー攻撃事例がメディアで取り上げられているが、SecHack365では、「研究倫理」「サイバーセキュリティに関わる実際の法律」「守られるルール、守られないルール」といった題材をテーマとして、ハッカソンによる研究技術開発だけではなく、セキュリティに関わる倫理や法制度に関する教育にも取り組んでいる。

6. おわりに

東京2020大会を控える我が国では、今後もますますセキュリティ対策の必要性と人材需要が高まることが予想される。NICTナショナルサイバートレーニングセンターでは、より効率的かつ効果的な演習等を提供すべく、各演習プログラムの構成や品質を常に高めながら今後の人材需要に応えていく予定である。

参考文献

[1]　情報処理推進機構、(2014年7月)、「情報セキュリティ人材の育成に関する基礎調査」報告書
https://www.ipa.go.jp/security/fy23/reports/jinzai/
[2]　内閣サイバーセキュリティセンター、(2015年9月)、サイバーセキュリティ戦略
http://www.nisc.go.jp/conference/cs/
[3]　経済産業省、(2016年6月)、IT人材の最新動向と将来推計に関する調査結果について
http://www.meti.go.jp/policy/it_policy/jinzai/27FY_report.html