5-5　Co-Nexus C: 演習基盤開放による国内セキュリティ人材育成事業の活性化

5-5　Co-Nexus C: Revitalize of Security Human Resource Development by Infrastructure for Training

佐藤 公信
SATOH Hironobu

DX を進めるにあたり、我が国では、セキュリティ人材不足が大きな問題となっている。組織において、セキュリティトレーニングにあてる予算を確保できないという問題がある。加えて、高度なトレーニングを設計運用できる組織は少なく、この問題もセキュリティ人材不足につながっているという声も聞こえてくる。そこで、Co-Nexus C では、トレーナーが容易に講習を実施できるクラウドシステム及び教材の作成し、広く我が国での利用可能な環境を構築する。これにより、高度な人材から組織でのプラスセキュリティ人材となり得る人材の育成、セキュリティ人材不足の解消の一助としての貢献を目指す。

In promoting DX, the shortage of security personnel is a major problem in our country. There is a lack of budget available for security training in some organizations. In addition, few organizations have capable of designing and operating advanced training programs, and some say that this problem is also linked to the shortage of security personnel. Therefore, Co-Nexus C will develop a cloud system and teaching materials that will enable trainers to easily conduct training courses and build an environment that can be widely used in Japan. This will contribute to the development of human resources who can become positive security personnel in organizations from advanced personnel and help to solve the security personnel shortage.

1　まえがき

我が国では、セキュリティ人材の不足が問題とされ、人材育成のためのトレーニングが課題である。ISC2 の調査 [1] によると、いまだ 11 万人のセキュリティ人材不足との調査がある。特にセキュリティについてトレーニングできる人材不足は、深刻な課題という声が聞こえてくる。セキュリティ人材といっても組織において必要とされるスキルセットが異なり、組織が求めるセキュリティ人材のスキルセットと自身のスキルセットにギャップがある [1]。組織は、トレーニングにより、ギャップを埋めようとするが、組織のトレーニングに費やす予算が不足しているという現実がある [2]。

このような課題を解決するため、CYNEX Co-Nexus C では、参画組織がコストを押さえつつ人材育成、トレーニングを始めることができる教材やオンラインで利用できる演習環境、それらに付随するシステムをプラットフォームとして開発及び運用を進めている。

人材育成に必要なコストとしては、演習環境を含む教材の開発、演習環境の維持、ニーズの調査と多岐にわたる。Co-Nexus C の活動を通して、これらセキュリティ人材育成に必要なコストを抑え、Co-Nexus C 参画組織の演習展開コスト低減をプロジェクトの目的としている。

基本的には、Co-Nexus C では演習を主催、トレーナーとして演習をすることはなく、参画組織での演習主催、実施としている。NICT が提供する演習環境を含む教材を Co-Nexus C 参画組織が、その組織内でトレーニングしても構わない、また、外部に販売しても構わない。ただし、外部に販売する場合は、参画要綱に基づきライセンス料の支払い義務が発生する。

2　Co-Nexus C の目指すところ

図 1 は、セキュリティ人材育成、特に教材を作成する際に必要と思われるコストを列挙し、それらコストを Co-Nexus C のどの活動により、低減するかが示さ

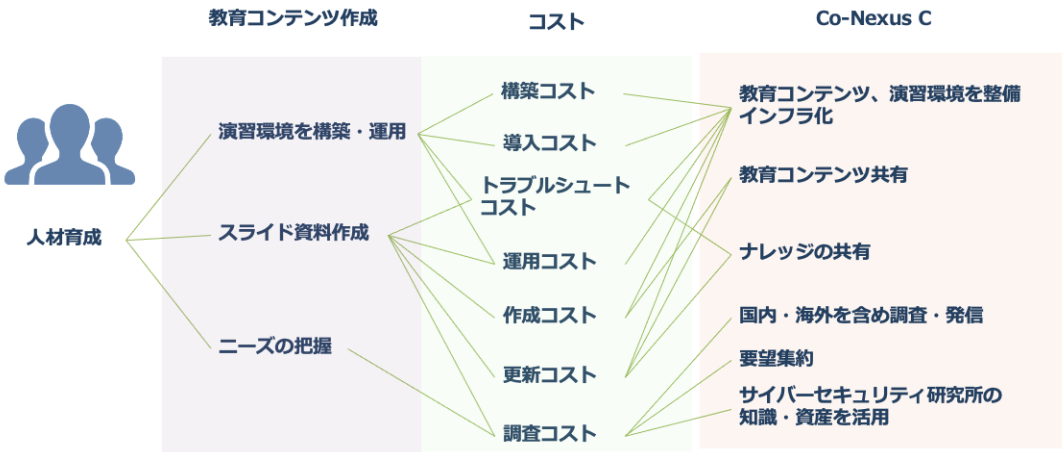

図 1　Co-Nexus C の活動

れている。コストとしては、開発から運用に至るまでのコストが列挙されている。演習環境の構築にかかるコスト、トレーニングのコンテンツを利用してトレーニングするために習得するために必要なコストや演習環境を運用する、また、陳腐化するコンテンツを更新維持するコストなどが挙げられている。Co-Nexus C の活動として、トレーニング環境のインフラ化を目指し、参画組織の演習環境構築コストやトラブルシューティングのコストを吸収するなど、セキュリティ人材育成に関わるコストを、Co-Nexus C の活動により吸収する。Co-Nexus C の活動により、Co-Nexus C に参画する組織が、セキュリティ人材育成にかけるコストをできるだけ低減し、金銭的、時間的、人的に導入コストを抑えセキュリティ人材育成を展開可能と考えている。

Co-Nexus C では、2021 年より、我が国のセキュリティ人材育成に資する各種教材、演習環境の開発、国内海外問わずセキュリティ教育に関する調査を実施している。セキュリティ教育に関する調査により、国内のニーズを把握する。さらに、国外でのセキュリティ教育に関する調査を実施し、先進事例を取り入れ、各種教材、演習環境の開発に生かしている。調査によりまとめられた情報は、ハンドブックとして公開される予定ある。

Co-Nexus C において NICT が開発し提供する教材としては、これまでナショナルサイバートレーニングセンターが作成したインシデントハンドリングをパソコンを使いながら学ぶことができる実践的サイバー防御演習（通称 CYDER）[3] 及びオリンピック事業者向けトレーニングとして整備された Cyber Colosseo の教材の一部が提供されている。

その他、CYNEX のオリジナルとなる教材、通称オリジナルコンテンツとして、SQL インジェクション、ペネトレーションテスト、IoT セキュリティ、パケットキャプチャなど、PC を利用しながら学べる教材の拡充を進めている。セキュリティ基礎として、OS の仕組みや、ネットワークルーティングを学ぶ教材も開発している。これら教材は、CYNEX Co-Nexus C へ参画することにより、利用することが可能である。また、スライド等の資料は、改変可能であり、トレーナーが目指すトレーニングを容易に実現できるライセンスとしている。

ここまで説明をしてきた教材は、トレーナーが付き教室やバーチャルクラスルームでオンラインとしてトレーニング提供に主眼を置いている。トレーナーを必要とせず、受講者が自己学習できる教材も開発し、Co-Nexus C 参画組織にて利用可能な教材としている。インシデントハンドリング及びフォレンジックを受講者自己学習できるもので、知識をインプットするパート及び仮想環境を用いて実際に応用するパートにより教材が構成され、Co-Nexus C の参画組織は NICT が開発した教材及び演習環境を NICT が規定するライセンスに基づき利用可能である。人材育成のエコサイクルとするため、Co-Nexus C の参画組織は、Co-Nexus C の参画組織が利用するために教材の持ち込みを可能としている。参画組織が持ち込む教材のライセンスは、持ち込み参画組織が自由に設定できる。教材の特徴や主な教材については、次章以降で詳しく説明を行う。

実践的で応用できる内容を学ぶためには、パーソナルコンピュータ（PC）を使い、手を動かして学ぶハンズオンの利用が望まれる。例えば、SQL インジェクションやペネトレーションテストなどを学ぶ際である。手を動かして学ぶためには、演習環境を準備する必要があるが、演習環境の構築に時間と経験、計算資源の準備といった様々なコストを要するため、応用につながる教育を実現するハードルは高いものがある。これらの問題を解決すべく Co-Nexus C では、SQL インジェクションやペネトレーションテストを学ぶための教材及び演習環境を提供し、我が国で利用可能なプ

ラットフォーム、インフラの構築を目指し開発を実施している。

3 教材の特徴

NICT が開発する教材の特色を示す。トレーニング後の受講者のスキルセットが明確なトレーナーにとって利用しやすい教材とするため、NICE Framework [4] を学べるものの基準として利用している。NICE Framework は、インシデントレスポンダーといった役割をなすために、タスクが割り当てられ、それぞれのタスクを実行するための Knowledge と Skill が関連付けられ、示されている。NICE Framework は、アメリカ政府のみならず、国家単位で共通化するためのフレームワークである。日本では、JNSA（日本ネットワークセキュリティ協会）が提供する SecBok [5] と互換性を有する。主に 3 つの特徴があるので、次に示す。

①トレーニング設計時にトレーナーが目指す、受講者のトレーニング後のスキルセットを実現が容易になるように、NICT で開発した各教材には、NIST NICE Framework が定義する Knowledge 及び Skill を関連付けている。

②各教材には、受講に際しての前提知識が設定されている。前提知識の提供は、講習対象の受講者に必要な前提知識がない場合、必要な前提知識をトレーニング中に補うための手助けとなる。教材の各パートに受講者が学べば身につく Knowledge 及び Skill について NIST NICE Framework を基にして設定されている。

③ NIST NICE Framework において定義ではないが、認知プロセスの次元について前提知識及び身に付く知識において指標を、タキソノミーテーブルを用いて示している。タキソノミーテーブルは、認知プロセスの次元を 6 段階（1. 記憶する 2. 理解する 3. 応用する 4. 分析する 5. 評価する 6. 想像する）としている。

オリジナル教材は、利用するトレーナーを情報処理安全確保支援士相当の知識を有する者が利用するとして、開発を進めた。各スライドのノート部分には、「伝える目標」「説明の流れ」「説明のポイント」が記載され、情報処理安全確保支援士相応の知識を有する者であれば容易に説明できる仕様としている。トレーニング中、よく受講者が間違うポイントやトラブルシューティングについて記載したトレーナー用のマニュアルも整備している。

これらのほか、トレーナーに必要な教授法のスキルセットとマインドセットを学ぶことができるトレーナーズトレーニングに関する教材も開発した。トレーナーズトレーニングでは、NICT が提供するオリジナル教材において、どのように教材を調整して利用するかの応用例まで身につけることができる。トレーナーズトレーニングもまた、参画組織で利用可能である。

4 NICT 提供教材

4.1 オリジナルコンテンツ

受講者に、より深い理解が進むために、オリジナル教材においては演習環境を提供している。提供する演習環境は、可能な限り利用する組織の導入コストを低く抑えるプラットフォームの開発を目指している。

オリジナルコンテンツ演習環境は、NICT において開発、運用がなされている。利用を希望する組織は、手順に従い利用申請し、演習環境が希望の期間利用可能となる。図 2 は、OT セキュリティを対象とする演習環境のイメージを示している。受講者は、Apache が提供する Guacamole を利用して、演習環境へ接続を実

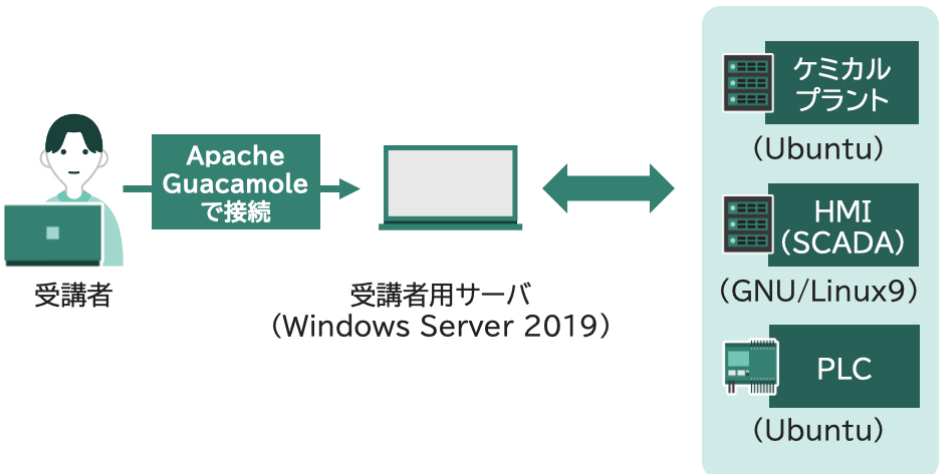

図 2　演習環境イメージ

施する。受講者は、Web ブラウザを利用することにより、演習環境へのアクセスの起点となる受講者用のサーバへアクセス可能である。受講者は、演習環境を利用するには、PC とインターネット利用が可能なネットワークを準備するだけである。受講者からみると、この演習環境は、クラウドサービスと言える。演習環境では、インターネットへ影響を与えないためファイアウォールにより通信制御がなされている。

4.2　SOC 人材育成コンテンツ

SOC（Security Operation Center）人材育成に特化、脆弱性診断士やフォレンジックアナリストのための自己学習用システムの開発も実施した。自己学習システムは、インターネットに接続できるネットワークに PC を接続し、Web ブラウザにて利用可能である。オリジナルコンテンツと同様に Web ブラウザを介して個人ごとに用意された演習環境にアクセスし、ハンズオンにより演習を実施する。

自己学習システムは、解説パートとハンズオンパートの 2 つのパートに別れている。技術的な解説をする解説パートでは、ハンズオンパートで実際に応用を行うために必要な知識の解説がなされる。解説パートでは、知識の確認を行えるように確認用のテストが用意されている。ハンズオンパートでは、解説パートで得た知識を応用するため、各個人が仮想マシンを起動し、ハンズオンを実施する。

教材の内容としては、インシデント時の初動対応から証拠保全といったインシデントレスポンス、フォレンジック、マルウェア解析、脆弱性診断である。

4.3　トレーナーズトレーニング

トレーニングのトレーナーを担う場合、受講者に教えるべき知識、また、教える、伝えるためのスキルが必要になる。例えば、事前に受講者の知識を把握しトレーニング資料を調整するスキル、コミュニケーションスキル、受講者からの信頼を得るためのスキルなどが教える、伝えるためのスキルセットである。Co-Nexus C では、トレーナーに必要な教示スキルセットやマインドセットを学べるトレーニングを開発した。組織内でのトレーナーの育成に利用することができる。

4.4　実践的サイバー防御演習

CYDER（実践的サイバー防御演習）は、インシデントハンドリングの一連の手順を体験することができるトレーニングである。受け付け・検知からインシデントケースクローズまでを PC ハンズオンを交えながら体験できる。これまで開発がなされてきた CYDER の一部コースが教材として Co-Nexus C から提供されている。

5　現状と今後の展望

現在、企業、高等教育機関、官公庁を含め 47 組織（2024 年 6 月 10 日現在）が、Co-Nexus C へ参画している。セキュリティトレーニング企業から高等教育機関まで、オリジナルコンテンツや自己学習システムの利用が進んでいる。一部の教材は、B2C（Business to Consumer）及び B2B（Business to Business）での商用での提供が進んでいる。「Based on the educational material developed by NICT」という表記があれば、その教材は、オリジナルコンテンツもしくは CYDER といった NICT が提供する教材を基にして作られた教材である。セキュリティトレーニングを受講される際は、是非、配付資料の最終ページなどで、「Based on the educational material developed by NICT」を探してみていただきたい。

地政学や技術トレンドの変様などの影響を受け、情報セキュリティ技術のトレンド変化や法律やガイドラインの改正や改訂が予測される。今後は、コンテンツの陳腐化を回避するために、更新作業を継続する予定である。更新作業とは相反し、可能な限り一貫した演習環境を維持し、トレーナーが新しい演習環境や教材の利用に当たっての導入コストを低減する予定である。

【参考文献】

1　ISC2,"How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce," 2023. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf
2　総務省,"令和 2 年版情報通信白書," 2020. https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd134530.html
3　NICT ナショナルサイバートレーニングセンター. CYDER https://cyder.nict.go.jp
4　https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center
5　日本ネットワークセキュリティ協会,"セキュリティ知識分野（SecBoK）人材スキルマップ 2021 年版," 2021. https://www.jnsa.org/result/skillmap/

佐藤 公信（さとう ひろのぶ）
サイバーセキュリティ研究所
サイバーセキュリティネクサス
CYNEX 研究開発運用室
主任研究員
博士（工学）
ニューラルネットワーク、パターン認識、画像処理
【受賞歴】
2021 年　文部科学大臣表彰　科学技術賞　理解増進部門