3.10.3.2 サイバートレーニング研究室

室長　　衛藤 将史　ほか5名

セキュリティ人材育成の未来を切り拓く

■概要

当研究室は、ナショナルサイバートレーニングセンター内において、サイバーセキュリティないしICTに係る人材育成事業であるCYDER（サイダー）、サイバーコロッセオ及びSecHack365（セックハック サンロクゴ）の演習及びプログラムの実施を主に技術的側面で支えつつ、当研究室固有の研究開発として、より効果的、効率的に演習事業を推進するための研究開発、他分野への応用に向けた技術開発及び外部への技術移転のための研究開発等に取り組んでいる。

セキュリティ人材不足が深刻な問題となっている現在において、１人でも多くのセキュリティ人材を迅速に育成する必要性から、セキュリティ人材育成を効率化し、その効果を最大化する必要性は非常に高いところ、当研究室は、その担当業務自体に存在する課題に直面しながら、その解決のための研究開発に取り組むという独自の立ち位置で業務を行っているところに、その特色と強みがある。

■平成29年度の成果

当研究室の成果につき、主としてCYDER等に関する研究開発結果を以下で報告する（SecHack365についても、当研究室のメンバーがトレーナーを務めているが、その成果は、当センターの報告のとおりである）。

1　CYDER及びサイバーコロッセオ演習内容の充実

セキュリティ人材育成の裾野を広めつつ、効果的な演習を行うためには、多様なニーズに応えることができる演習シナリオを作成し、これを全国展開していく必要がある。このため、当研究室においては、平成29年度に実施したCYDERについて、従来の地方公共団体及び国の行政機関等向けの中級レベルの演習（Bコース）に加え、全国47都道府県に展開される初級レベルの演習（Aコース）を新設して各受講対象者に応じたシナリオを用意した上、NICTが有する大規模サーバー群「StarBED」に演習用の仮想環境を構築するなどして演習環境を整備し、前年度比で約２倍の受講者に演習を実施した。

また、東京2020オリンピック・パラリンピック競技大会においては、大会関係組織に対し、より高度なサイバー攻撃がされることが予想されるところ、これに対応するための演習であるサイバーコロッセオでは、準上級コースを設け、「攻防戦」を取り入れた高度な演習シナリオを作成し、演習を実施した。

この「攻防戦」は、サイバー攻撃を行う側の手口や行動等を自らが体験することにより、その知見を防御に生かすことを特徴とする非常に実践的かつ高度な演習方式（図１）であるが、その演習効果が高い反面、最新のサイバー攻撃に関するデータセットやその知見が必要であるうえ、演習環境構築が困難かつ大きなコストが掛かるなどの課題があることから、我が国では普及が進んでいるとは言えない状況にある。当研究室では、NICTが有するStarBED及び長年のサイバーセキュリティ研究による技術的知見を活用することにより、前記課題を解決し、攻防戦を取り入れた実践的サイバー防衛演習シナリオを実施した。

2　CYDERANGE（サイダーレンジ）の開発

セキュリティ人材育成事業を効率的・効果的に推進するためには、演習環境の運用性を向上させつつ、演習実施に係る費用を可能な限り低減させた上、演習効果をより高めるための良品質な演習シナリオを作成し、受講者のスキルに応じてこれを提供する必要があるが、これに関しては次のような課題が存在した。

まず、従前のサイバー演習では、演習プログラムを作成・変更する都度、シナリオや演習環境を手作業で更

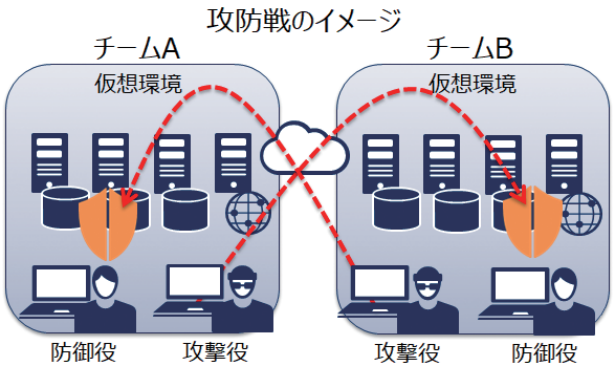

図1　攻防戦のイメージ

新・再構築することが一般的であったが、これらの作業には膨大な時間・労力・費用が掛かるという問題があり、CYDERのような大規模な演習事業においては、シナリオ作成や環境構築に伴う作業を可能な限り自動化していくべきことが課題となっていた。

また、受講者のレベルと演習内容のミスマッチを解消し、演習効果を高めるという観点では、従前のように、既に用意された演習シナリオから、受講者が自らのレベルに合っていると考えるものを主観的に選択して受講するよりも、客観的に各受講者が有するスキルに適合した内容の演習シナリオを、演習実施側が選択して提供する必要性があったが、その前提となる各受講者のスキルや学習効果の判定等には非常に困難な問題を伴い、大きな課題となっていた。

今回、当研究室は、上記課題を解決するため、これまでのCYDERの事業運営を通じて得られた知見とNICTが有するサイバーセキュリティ研究に関する技術を活かし、演習シナリオの自動生成及び演習環境の自動構築等を可能とする演習自動化システム「CYDERANGE」を開発した。

このCYDERANGEの特徴は、以下のとおりである（図２）。

・フライトシミュレーター等でも用いられる次世代の演習データ記録方式の世界規格Experience APIに準拠し、演習環境における受講者のあらゆる操作情報を記録し、分析することで、演習品質の向上が可能
・受講者のプロファイル（スキルレベルや業務領域等）に合わせて、最新事例を踏まえたサイバー演習シナリオの自動的生成が可能なほか、生成されたシナリオの舞台となる演習環境をも自動構築することが可能
・受講者のプロファイルに合わせた効果的な演習プログラムを短時間で作成することが可能
・演習内容及び演習環境の自動構築化機能により、演習運営に掛かるコストを大幅に削減

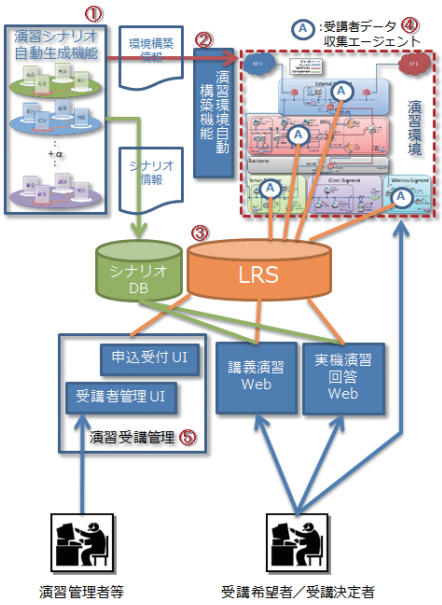

図2　演習自動化システムのイメージ

なお、演習環境上では演習効果の向上を目的として、データ収集エージェントが、受講者が演習受講に関連してとったあらゆる行動（キー入力、マウス操作及びウィンドウ操作等の演習受講に伴う操作等）をパーソナルデータの適切な取扱いに十分配慮しつつ収集し、データベースに蓄積したうえ、今後、これによって得られた膨大な受講者データを機械学習等の技術によって分析することで、演習による学習効果を精密に測定することが可能となる予定である（本分析機能は平成31年度以降に実用化予定）（図３）。

当センターでは、平成30年度からCYDER事業においてCYDERANGEの本格運用を開始し、金融、交通インフラ及び医療等の分野ごとに、きめ細かく最適化されたサイバー演習環境等を、迅速かつ低コストに開発・運用する予定であるほか、CYDERANGEの運用によって得られた膨大なデータを分析することにより、今後の演習事業における、より一層の品質向上と効率化を予定している。

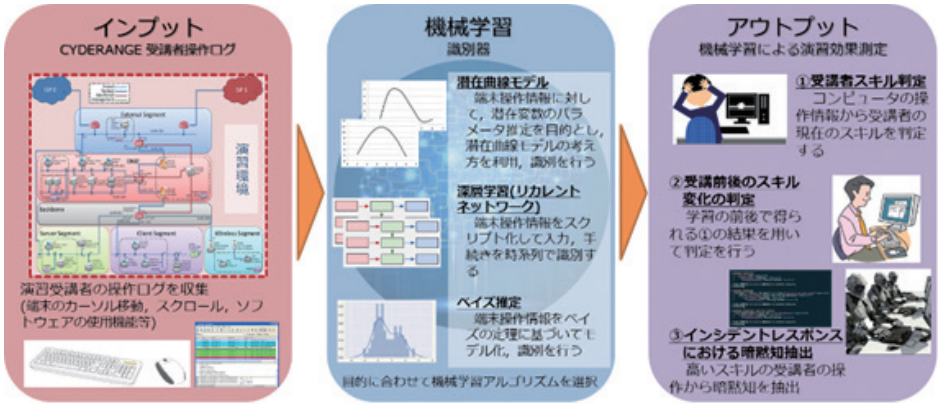

図3　演習効果自動測定のイメージ