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12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 30 年度の成果

１．CYDERANGE（サイダーレンジ）の実運用開始

当研究室は、平成29年度までに、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、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。

なお、このCYDERANGEの特徴は、以下のとおりである（図１）。

- 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、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
- 演習内容及び演習環境の自動構築化機能により、演習運営にかかるコストを大幅に削減

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・運用したほか、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。

また、当研究室では、CYDERANGEの効果を最大化すべく、平成30年度から、CYDER演習の学習効果を客観的に評価できる技術を確立するため、3,000人以上に及

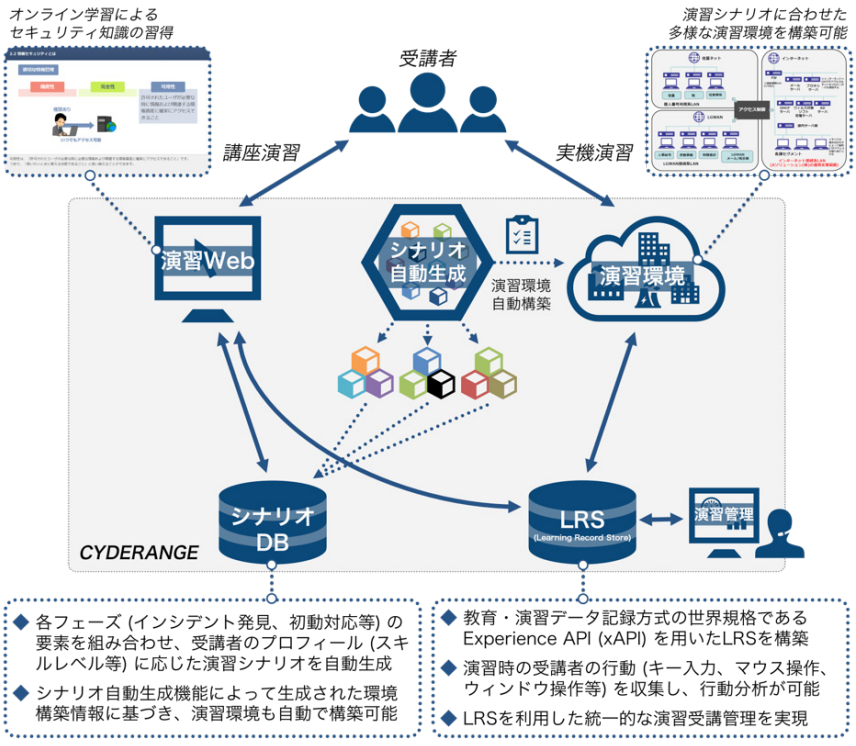

図1　CYDERANGEのイメージ

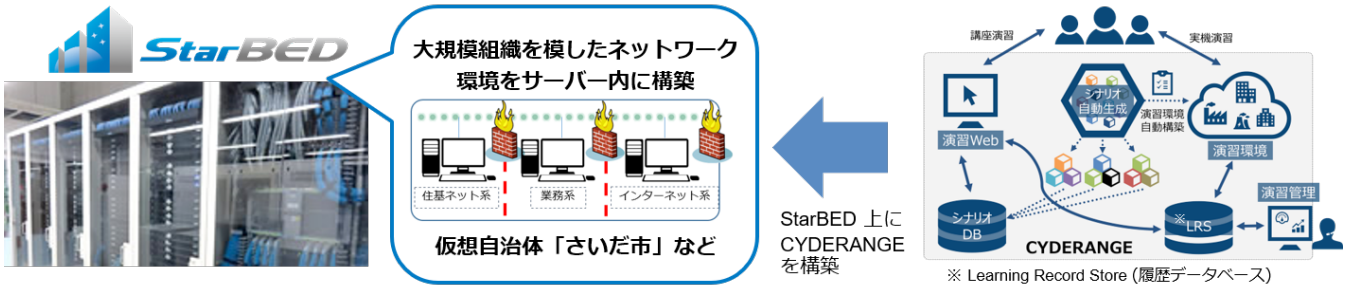

図2　CYDERANGEの活用イメージ

ぶ受講者が行った様々な活動ログを、数理的アプローチにより定量的に測定し、受講者属性に応じた学習効果の分析等を可能にするための手法に係る研究に着手した。

2．CYDER演習内容の拡充等

当研究室においては、平成29年度、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、これを実施した。

さらに、平成30年度は、重要社会基盤事業者向けのB-3コースを新設した。同コースのシナリオは、金融、交通インフラ、医療、教育研究機関、一般等の分野別に細分化しているところ、当研究室が実運用を開始したCYDERANGEを活用することにより、分野ごとにきめ細かく最適化した演習環境等を、迅速かつ低コストに開発・運用することが可能となった（図２）。

そして、CYDER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、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。

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（本分析機能は令和２年度以降に実用化予定）。

3．サイバーコロッセオの実施

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、準上級コースにおいて、「攻防戦」を取り入れた高度な演習シナリオに基づく演習を実施した（図３）。

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か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い難い状況にある。当研究室では、平成30年度においても、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。

4．SecHack365の実施

平成29年度から開始された若手セキュリティイノベーター育成事業であるSecHack365では、当研究室のメンバーの多くがトレーナーを務めており、平成30年度においても、選抜された50名のトレーニーに対し、NICTが有する遠隔開発環境「NONSTOP」及び研究・開発に関する知見や人的資源という強みを活用することにより、他に類を見ない、１年を通して行われる、アイデアソン・ハッカソン、遠隔研究・開発、発表の組み合わせによる総合的能力開発プログラムを実施した。

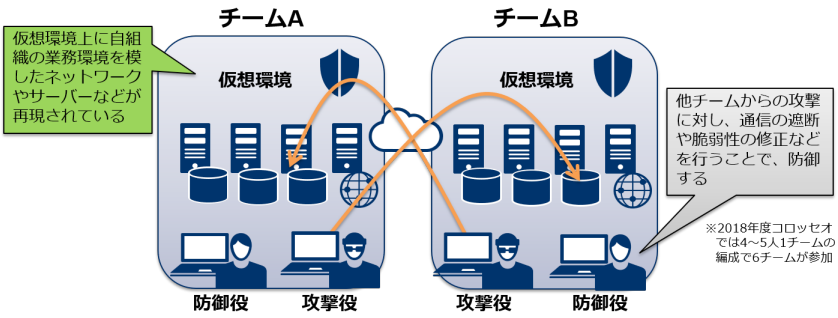

図3　攻防戦によるサイバー演習イメージ