5F-07

サイバー攻撃と防御に関する コンテナ方式による仮想型演習システム CyExec の開発

中田　亮太郎†　長谷川　久美†　瀬戸　洋一†

公立大学法人首都大学東京　産業技術大学院大学　産業技術研究科†

１．　はじめに

情報セキュリティへの対策は社会にとって大きな課題になっている[1]．人材の不足が懸念され，実践的な教育環境の整備が求められている[2]．

一部の高等教育機関では，市販のサイバーレンジを導入した教育や，企業と連携したサイバー攻撃と防御の教育を実施しているが，導入や維持管理に多大なコストがかかり，多くの教育機関での整備には限界がある．

そこで，導入運用コストやポータビリティに優れた教育環境の実現方式を提案し，多くの大学や企業等で実践的な教育環境を整備できる方法を検討した．

本稿では，検討した仮想型演習システム「CyExec（Cyber security ExerCise）」の概要と，それを用いた演習レベルの設定方式を説明する．

２．　サイバー攻撃と防御教育の課題

２．１　サイバーレンジによる教育

サイバーレンジとは，実環境を仮想空間におけるサイバー攻撃と防御の演習場として，サイバー攻撃への備えや対応などを体験するシステムである．受講者のスキルレベル等によって，攻撃の検知確認，監視ツールを用いて収集したログから痕跡を見つけることや，さまざまな種類のデータ分析手法を利用して悪意のある活動を検知するなど，広範囲のシナリオ設定が可能である．

２．２　サイバーレンジ教育の課題

サイバーレンジを用いた教育は，専門カリキュラムを組む一部大学や，NICT（情報通信研究機構）・IPA（情報処理推進機構）等の専門機関により，企業等と連携するなどして実施されている［2］．導入や維持管理，カスタマイズ等には，専門の教員による指導や企業等との協業が必要となり，多大なコストが必要となる．そのため，その教育効果には期待が見込めるものの，多くの教育機関でサイバーレンジを整備するには限界がある．

サイバー攻撃・防御に関する学習や，オープンソースを用いた演習環境の構築に関する研究を行う大学もあり，コストを抑えつつ教育効果のある演習環境が望まれている[3]．

３．　演習システムの提案

３．１　演習環境の検討

演習シナリオの追加や改変に柔軟に対応し，かつ物理的な構成に縛られないことで導入の容易さを確保する，VirtualBox や Docker などの仮想化技術による演習環境を受講者の PC へ実装する．演習室などの既存の学習環境への影響を最小限とし，移植性・拡張性にも優れたシステムを考慮する．

VirtualBox はホスト型ハイパーバイザと呼ばれる方式で，Windows や MacOS 上でアプリケーションとして別の OS（ゲスト OS）を稼働させる．この場合，演習シナリオに応じて必要な数のゲスト OS が稼働する環境を用意し，それぞれで攻撃や防御用のプログラムを動作させるなど，演習シナリオ１つに対して複数のゲスト OS を用意する必要があり，ホスト側のディスク容量やリソースの消費の大きさが課題である．

一方，コンテナ型である Docker は，ホスト OS 上でコンテナと呼ばれる専用領域を作り，その中で必要なアプリケーションを動作させる．ディスク容量やリソースの消費はごく少量であるが，提供できるホスト OS の種類の少なさや，動作環境の違いなどによる環境の配布の難しさなどを考慮する必要あるなどの課題がある．

演習環境は VirtualBox と Docker それぞれの課題に対処し，構築の容易さと展開・配布などの容易さを考慮した融合環境を提案した．図１に概要を示す．

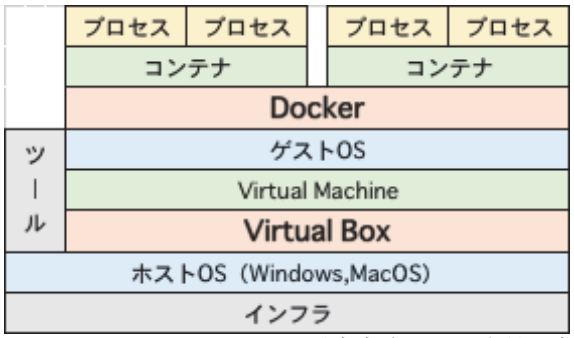

図１ VirtualBox と Docker の融合方式による演習環境

融合型の演習環境では、VirtualBox 上のゲスト OS で Docker コンテナを使用して攻撃や防御のプログラムを動作させる．コンテナが動作するゲスト OS のイメージを配布することで、環境の構築と配布の容易さを両立させることが可能となる．

３．２　学習スタイルの検討

演習環境を用いた学習スタイルは，受講者が利用する PC 上で完結する自己完結型と，指導者と受講者，もしくは受講者同士が攻撃側と防御側に分かれるインタラクティブ型がある．

自己完結型は環境の準備・配布が容易であるが，基本的に攻撃や防御の操作を受講者が決められたシナリオに沿って行うため，リアリティに欠ける．一方，インタラクティブ型はより実世界に近い演習が可能であるが，運用時における安全性確保を考慮し，閉じたネットワーク内で運用するなどの注意が必要である．

Development of Container-based virtual exercise system CyExec related to cyber attack and defense
†Ryotaro Nakata,Kumi Hasegawa,Yoichi Seto,
Advanced Institute of Industrial Technology

Copyright ©2018 Information Processing Society of Japan.
All Rights Reserved.

演習環境の開発は，最初のステップとして自己完結型の環境を完成させ，発展的にインタラクティブ型の環境や IoT デバイスを含む実世界に近い環境を検討する．

4． レベル設定と学習内容

4．1 演習プログラムの課題

演習プログラム開発にあたり，レベルの定義方法と求められるスキルが不明確であった．この課題に対し，組織のセキュリティ対策における方法論である Threat Hunting の概念を用いて検討した．図 2 に概要を示す．

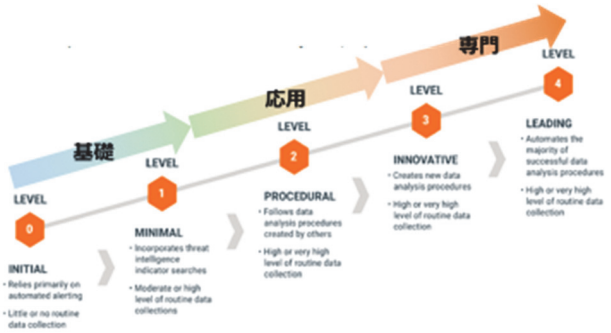

図 2 Hunting Maturity Model(HMM)とレベル定義

Sqrrl 社が提唱する Hunting Maturity Model(HMM)は，Threat Hunting において組織が行うべき内容を段階的に示しており，ハンティングチーム構築・改善の際の指標となる[4]．

受講者の技術や知識レベルを HMM の定義と対応させ，目指すべきレベルを確認する．レベル毎に必要なスキルを明確にするため，SANS が提唱している SOC 業務の役割と HMM のレベル定義を対応させた[5]．表 1 は SOC 業務の役割と対応する HMM レベルを示す．

表 1 SOC 業務と対応するレベル

SOC業務	対応するレベル（Hunting Maturity Model）				
	レベル0	レベル1	レベル2	レベル3	レベル4
アラート分析者	○	◎	○		
インシデント対応者			◎	◎	○
専門家				◎	○
SOC責任者				○	◎

SANS は SOC 業務に必要な学習内容を示している．より詳細なスキル内容を把握するため，JNSA が公開している SecBok 人材スキルマップで用いられている役割一覧から，SOC 業務の内容に対応するものを選び，役割ごとに必要なスキル項目の詳細を抽出する．表 2 にスキル例を示す．

表 2 演習プログラムに必要なアラート分析者のスキル例

学習内容	対応するスキル項目（SecBok2017）
データ収集	・ネットワーク保護コンポーネントの設定と利用に関するスキル ・センサのチューニングに関するスキル
脅威情報の参照	・現在及び新興の脅威/攻撃手法に関する知識 ・システムとアプリケーションのセキュリティ上の脅威と脆弱性に関する知識 ・脆弱性の種類と関連するカテゴライズに関するスキル
ツールを用いた基本的な調査	・ソフトウェアの通信上の脆弱性を識別するためのネットワーク解析ツールの利用に関するスキル ・システム/ソフトウェアの脆弱性を識別するためのエクスプロイトツールの利用に関するスキル ・システム診断ツールと障害識別技法に関する知識 ・ペエトレーションテストの原理、ツール及び技術 ・マルウェア解析ツールに関するスキル

4．2 レベル設定方式の提案

演習プログラムは，受講者のレベルや必要となるスキルの内容に応じて詳細な内容を検討する．レベルの決定は，HMM の内容に応じ目指すべきレベルを確認する．必要となるスキルの内容は，対象者を SOC の業務内容と対応させ，Hunt Matrix（Threat Hunting 業務の各フェーズにおいて何ができているべきかを段階別に示したもの）の内容や SOC 業務に必要な学習内容から確認し，対応する SecBok の役割別に示されている必須スキル小項目の中から抽出する[6]．

4．3 基礎レベルの演習プログラムの設定

考察したレベル設定方式に従い，基礎レベルの演習プログラムの仕様を決める例を示す．目指すべきレベルに対応する必要なスキルの詳細を，SecBok のスキル小項目から抽出し，演習の流れ（シナリオ）とプログラムの内容を考察する．例として XSS（クロスサイトスクリプティング）を題材とした演習プログラムの内容とスキル項目を示す。

① 正常な動作の確認や攻撃方法の推測： 現在及び新興の脅威/攻撃手法に関する知識，脆弱性の種類と関連する攻撃の認知とカテゴライズに関するスキル
② XSS の攻撃の方法，実際の動作の確認： システムとアプリケーションのセキュリティ上の脅威と脆弱性に関する知識
③ 脆弱性検査ツールで脆弱性の発見： システム/アプリケーションの脆弱性を識別するためのエクスプロイトツールの利用に関するスキル

5． おわりに

サイバー攻撃の増加やセキュリティ人材の不足に伴い，実践的な教育環境の整備が求められている．

提案したサイバー攻撃と防御の演習フレームワークは，仮想環境を用いることによる導入の容易さや，移植性，発展性にすぐれ，教育機関における協働化も視野に入れた利用ができる．

今回基礎レベルの演習プログラムを作成したが，レベルや学習内容の設定方法を提案したことにより，様々なレベルの受講者に必要となるスキル項目を明確化し，新たな演習シナリオやプログラム開発の際の指標として活用できる．

謝辞

本研究を進めるにあたり，本学 Project Based Learning チームメンバーの協力を得た．ここに感謝の意を表します．

参考文献

[1] “サイバーセキュリティ基本法“(2014 年 11 月 12 日法律第百四号)
[2] IPA, ”情報セキュリティ白書 2017” (2017.7.1)
[3] Razvan Beuran, Cuong Pham, Dat Tang, Ken-ichi Chinen, Yasuo Tan and Yoichi Shinoda, ” CyTrONE: An Integrated Cybersecurity Training Framework ”(2017)
[4] Sqrrl, ”A framework for Cyber Threat Hunting”, Sqrrl Data,Inc (2016)
[5] SANS Institute, “Building a World-Class Security Operations Center: A Roadmap ”(2015)
[6] JNSA, ”SecBok 人材スキルマップ”(2017.8.21)

Copyright ©2018 Information Processing Society of Japan.
All Rights Reserved.