エコシステムで構成するサイバー攻撃と防御演習システム CyExec の提案

豊田 真一[†1]　中田 亮太郎[†2]　長谷川 久美[†1]　慎 祥揆[†1]　瀬戸 洋一[†1]

概要：　サイバー攻撃は活発化かつ高度化している．対応するセキュリティ人材は不足し，人材育成が急務となる中，実践的なシナリオ型演習システムの開発が必要である．しかし，市販の演習システムは導入コストが高いため，高等教育機関や中小企業で利用することは難しい．これらの課題に対して，仮想化技術を利用した環境上に，演習プログラムを実装するシステムを開発することで解決する方針とした．本稿では，高等教育機関や中小企業で導入が容易な VirtualBox，Docker を利用した演習環境に，演習プログラムの共同開発が可能なエコシステムの考え方に基づくサイバー攻撃と防御演習システム CyExec を提案する．

キーワード：エコシステム，仮想化技術，サイバー攻撃と防御，情報倫理，セキュリティ人材教育

Proposal of Cyber attack and defense Exercise system CyExec composed of ecosystem

Shinichi Toyoda[†1]　Ryotaro Nakata[†2]　Kumi Hasegawa[†1]
Sanggyu Shin[†1]　Yoichi Seto[†1]

Abstract: Cyber attacks are becoming active and sophisticated. There is a shortage of security human resources corresponding to Cyber attacks, and human resource development is an urgent task in Japan. Although it is necessary to develop a scenario-type exercise system that can be practiced, it is difficult to introduce commercially practiced exercise system at Higher education institutions and small and medium-sized enterprises because the installation cost is very high.

To solve these problems, we resolved policy to resolve by developing an exercise system that implements exercise programs on the environment using virtualization technology. In this paper, we propose Cyber attack and defense exercise system "CyExec" based on the concept of an ecosystem which can jointly develop exercise program in practical environment using VirtualBox, Docker which can be easily installed by Higher education institution and small and medium-sized enterprises.

Keywords: Cyber attack and defense, Ecosystem, Information ethics, Security human resources training, Virtualization technology

1. はじめに

各国でサイバー攻撃によるインシデントの発生件数が増加し，社会的な影響が表面化している．日本でも 2015 年 5 月に発生した年金機構の情報漏えい事件をはじめ，2018 年 1 月の仮想通貨流出事件など，生活に直結する事件が発生し，サイバーセキュリティに対する社会の関心やニーズが高まっている[1].

政府のサイバーセキュリティ戦略では，セキュリティ人材の育成が課題となっている．例えば，2020 年には 19 万人以上の人材不足や，セキュリティ業務に従事する人材でも知識・スキル不足が懸念されている [2][3].

セキュリティ人材育成の取り組みとして，一部の大学や公的機関ではサイバーセキュリティの知識・技術を修得するため，専用のアプリケーションを用いた脆弱性やサイバー攻撃と防御を体験する演習が実施されている[4][5].

市販のサイバーレンジによる演習では，仮想環境に構築されたネットワーク上で，現実で起こる攻撃を想定した防御, 脆弱性への対応をチーム演習の形式で体験学習できる．また，実際のマルウェアを用いるなど，現実に起こりうるシナリオを利用して，役割に応じた組織的な対応方法を学ぶことができる．このため，高い教育効果が期待できる[6][7].

しかし，大学などの高等教育機関では，導入コストの問題や，演習環境の維持管理を行う人員の不足から，高度なセキュリティ人材を育成するための教育環境の整備は進んでいない．演習プログラムやカリキュラムを協力して開発可能で，導入が容易なサイバー攻撃と防御の演習システムの整備が必要である．

また，演習を通じて得られる技量には攻撃手法が含まれる．受講者が，演習により得た技量を，故意あるいは過失

†1 公立大学法人首都大学東京　産業技術大学院大学
Advanced Institute of Industrial Technology.
†2 学校法人　昭和女子大学
Showa Women's University.

により悪用し，攻撃側となるリスクがある．このため，受講者に対し攻撃と防御の技量を教えるだけではなく，法・倫理教育が必須である．

本稿では，高等教育機関や中小企業で導入可能なサイバー攻撃と防御の仮想型演習システム Cyber security ExerCise（以下 CyExec）を提案する．高等教育機関とは情報工学系の大学院を想定している． 2 章で既存演習システムの課題から CyExec の要求事項を示す. 3 章にてエコシステムの考え方をベースとする仮想型演習システム CyExec の提案，法・倫理教育のカリキュラム，および 4 章で CyExec 実装例を紹介する．

2. サイバー攻撃と防御の演習の課題

2.1 既存演習の特徴

表 1 に既存のサイバー攻撃と防御に関する演習の特徴を示す．サイバーセキュリティに関する代表的な演習として脆弱性診断とサイバーレンジがある．

表 1　既存のサイバー攻撃と防御に関する演習の特徴

	脆弱性診断	サイバーレンジ
代表的な演習プログラム、製品	WebGoat（OWASP Foundation） AppGoat（IPA）	CYBERIUM（富士通） TAME Range（DNP） CyTrONE（JAIST）
演習環境	受講者PC（ローカル環境）	クラウド，サーバ （仮想ネットワーク環境）
内容	脆弱性の原理，検知，影響度，対策についての演習	インタラクティブな攻撃と防御の演習
効果	脆弱性の体験を通じた理解	セキュリティインシデントに対する技術的，組織的な実践的対応力
費用	基本的には無償	一般的には数億円

(1) 脆弱性診断演習

脆弱性の検出，影響度，および対策について学習する．脆弱性診断プログラムは無償版が公開されている. 例えば，OWASP（Open Web Application Security Project）が提供する WebGoat，IPA（情報処理推進機構）が提供する AppGoat がある[8][9]．演習プログラムを受講者自身の PC にインストールすることで，演習環境の構築が可能である．

AppGoat は，Windows 上にのみ実装可能である．利用にあたっては，IPA に利用許諾条件合意書を提出する必要がある[10]．合意書には，「反社会的利用等を防止するため，本合意書は，利用者に高度の責任を求めています.」と記載され，合意した者のみがインストール可能となる．

「ウェブアプリケーション用学習ツール(集合学習モード) のみ，集合教育目的に有用と認める範囲で本製品を改変することができます.」と記載があり，ある程度のカリキュラム変更には対処できる柔軟性がある．また，解説資料など教材も整備されている[6].

受講者は，演習プログラムを利用し，サイバー攻撃に関係する脆弱性の検知，対策方法を修得できる．しかし，脆弱性診断は，組織的な対応方法は学習範囲外である．攻撃と防御というインタラクティブさに欠け，静的な脆弱性検出および対策に限定される．また，WebGoat の場合は，プログラム素材のみの提供であり，演習テキストが用意されていないため，演習実施にはカリキュラム，教材の整備が必要である．

(2) サイバーレンジ演習

セキュリティインシデントに対応可能な組織的人材育成を目的とした演習である．演習環境は，仮想環境上にクライアントやサーバ，ネットワークなど，実世界を模して構築される．

受講者は，マルウェアなど不正なプログラムを用いた攻撃に対し，攻撃手法やマルウェアの種類，被害状況や対応方法の確認を行うなど，攻撃発生から対応終結までの想定訓練が可能である．攻撃に対する防御技術と，CSIRT（Computer Security Incident Response Team）や SOC（Security Operation Center）などの組織的な対応手法も修得できる[7].

しかし，サイバーレンジは，高額な導入維持コストが必要である．高等教育機関側の意向に合わせたカリキュラム変更の柔軟性にも欠ける．また，演習環境の維持管理を行う専門人材を確保する必要がある．

高等教育機関では，現有する計算機環境で，脆弱性の対策および組織的な対応の基礎を修得できるカリキュラムが求められる．しかし，脆弱性診断は，攻撃と防御のインタラクティブ性に欠け，組織的な対応が不足する．一方，サイバーレンジは予算や人員に制約のある高等教育機関では導入が困難である．また， カリキュラム策定の自由度が小さい．次節で課題に対する対策方針を述べる．

2.2 演習における課題と CyExec に対する要求事項

表 2 は CyExec に実装する演習プログラムの学習範囲を示す.

表 2　CyExec で実現する演習

	脆弱性診断	サイバーレンジ
対象	• システムやアプリケーションの脆弱性	• 導入しているセキュリティ機器 • インシデントに対応するセキュリティ担当者
目的	• システムやアプリケーションの脆弱性の有無と影響度、検出方法の修得	• 組織全体のサイバー攻撃に対する耐性の調査 • インシデント時におけるセキュリティ担当者および組織の対応方法修得

CyExecの範囲
・脆弱性の検出、対策（脆弱性診断）
・CSIRT-SOCを想定した組織的な対応（サイバーレンジの一部）

高等教育機関における演習システムは，下記に示す内容を学習することが必要である（表 2 の点線部分）.

(a) 基礎技術として脆弱性診断（脅威と脆弱性の理解）
(b) 応用技術としてインタラクティブな攻撃と防御技術
(c) 組織的対応の基礎

CyExec は, 高等教育機関が現有する計算機環境を利用し，脆弱性の検出と対策技術の修得，インタラクティブな攻撃

と防御の基礎，および CSIRT や SOC などの人材育成を考慮した組織的対応の基礎を修得できる学習範囲を要求事項とする．

表 3 は演習における課題と対策を示す．

表 3　演習における課題と対策

	課題	対策
演習システム	高額な導入・保守コスト	現有計算機環境下で運用可能な仮想化技術を採用
	受講者のレベルに合わせたカリキュラムの整備は，単独の教育機関では困難	複数教育機関での共同開発，共同利用が可能なコンテナ技術を採用
法・倫理教育	受講者に誓約書の必要性，問題の影響度を説明していない	技術を間違って利用した場合の法的課題について，事前に教示

（1）　演習システム

高額な導入維持コスト，専門人員の確保が必要である．演習の実施には，受講者のレベルにあわせた技術的，組織的なカリキュラムを整備する必要があるが，単独の高等教育機関では困難である．

演習環境は，高等教育機関の現有計算機環境上で演習可能な仮想環境構成とする．また，複数の機関による連携を実現するため，移植が容易なコンテナ技術を用いる．

（2）　法・倫理教育

受講に当たって誓約書を求める組織が一般的であるが，必ずしも”なぜ誓約事項を遵守しなければならないか”を説明していない．

受講者が演習を通じて得た技量を，故意あるいは過失により悪用する場合があるため，受講者に対し，得られた技量の扱い方により法律に抵触することを，倫理を含め教育する．特に社会人経験のない学生への教育は必須である．

次章にて CyExec の構成および法・倫理教育カリキュラムの提案を行う．

3. 仮想型演習システム CyExec の提案

3.1 エコシステムとしての実現

エコシステムとは，単独の組織ではなく，関連する組織の協業により，業界全体が発展していくことを示す言葉である[11].

セキュリティ分野の技術の進展は早く，演習プログラムの開発には高い専門性と時間が必要である．したがって，演習プログラムの開発は，単独の高等教育機関で全てを完結することは困難なのが実態である．複数の高等教育機関や民間企業が連携し，演習プログラムを開発する必要がある．CyExec にエコシステムの考え方を導入し，複数機関での演習プログラム共同開発を実現する．

次節に具体的な実現方法を述べる．

3.2 演習環境の提案

（1）低コストで実現する演習環境

演習システム導入・維持管理にかかるコストの多くは，機器の費用とソフトウェア等のライセンス費用である．これらのコストを抑制し容易に環境構築するため，高等教育機関の現有計算機環境（クライアント PC, サーバー等）で，開発した演習を容易に実装利用できる仮想化技術を用いた演習環境構成を提案する．仮想環境構築には VirtualBox を利用する[12].

VirtualBox は，Windows や MacOS 上でアプリケーションとして別の OS（ゲスト OS）を稼働させることができ，高等教育機関の現有計算機環境上で演習環境の実装を実現する．

（2）　共同開発・共同利用が容易な演習環境

複数の高等教育機関による共同開発，共同利用を実現するためには，異なる機関間であっても演習プログラムを容易に開発・利用できる必要がある．このため，コンテナ技術を用い高い移植性を実現する．コンテナ技術は Docker を利用する[13].

VirtualBox にて構成したゲスト OS に Docker をインストールし，Docker 上にコンテナを設置する．脆弱性診断の動作のほか，攻撃や防御に関する機能を持った様々な自主開発のプログラムをコンテナで稼働させることで，目的別の演習環境を容易に構築できる．

Docker は作成済みのコンテナをクラウド上で共有する DockerHub というサービスがある．例えば，公開されているコンテナを利用すれば，簡単に Web サーバを構築できる．また，作成した演習プログラムを実装したコンテナを公開し，共同利用することができる．

さらに，CyExec 上に，多様な演習プログラムを共同利用する環境が整備されることで，複数の演習プログラムを組み合せた演習カリキュラムの開発，利用が可能となる．

図 1 は CyExec 演習システムのアーキテクチャを示す．

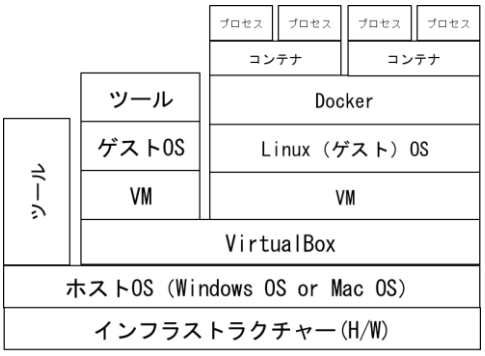

図 1　CyExec 演習システムのアーキテクチャ

提案する演習システムのアーキテクチャは，ホスト OS 上の VirtualBox で稼働するゲスト OS に Docker をインストールし，攻撃や防御のプログラムが動作するコンテナを Docker 上に実装する．これにより，VirtualBox のもつ現有計算機環境で動作可能な可搬性と，Docker コンテナの高い

移植性による演習プログラムの共同開発，共同利用を可能とする．つまり，CyExec はエコシステムを実現する演習システムである．

3.3 開発ロードマップ

サイバー攻撃手法は常に変化しており，CyExec は最新の攻撃シナリオに対応できることが求められる．したがって，CyExec 開発は，3 つのステップに分けて拡張を行い，多様な演習シナリオに対応できるように計画している．

下記に CyExec の開発ロードマップを示す．

(1) 自己完結学習型

図 2 は自己完結学習型の演習環境イメージを示す．

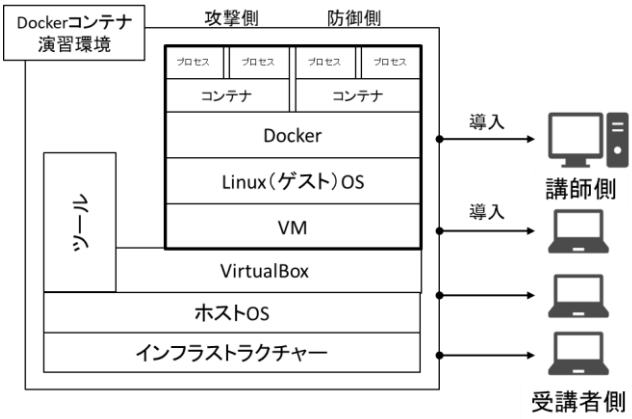

図 2 自己完結学習型の演習イメージ図

自己完結学習型の演習環境では，演習用の仮想マシンをユーザ（講師と受講者）の環境に導入し，自己完結型の学習スタイルをとる．教室などの対面学習の場合，講師側と受講者側は別々の PC を使用するが，画面や操作，および結果が同じになる．

(2) インタラクティブ型

図 3 はインタラクティブ型の演習環境イメージを示す．

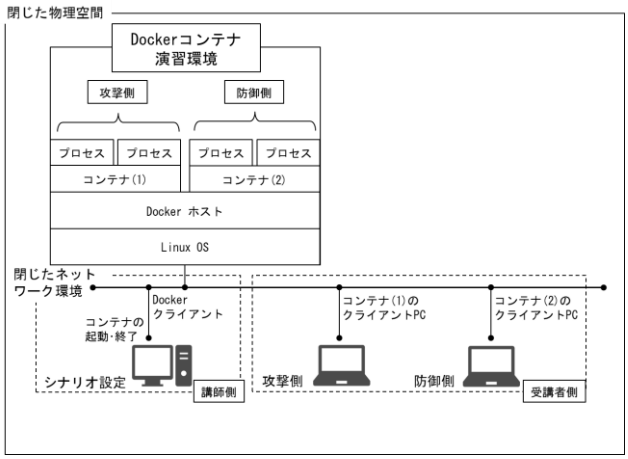

図 3 インタラクティブ型の演習イメージ図

インタラクティブ型の演習環境では，外部と接続しない閉じたネットワーク環境を用意し，ネットワークを経由して，Docker コンテナを操作する環境を構築する．攻撃側のコンテナを操作する攻撃担当の受講者，防御側のコンテナを操作する防御担当の受講者，それぞれの操作を分離することでインタラクティブな学習スタイルを実現し，実世界に近いシナリオに対応することが可能となる．

(3) IoT デバイスを接続した演習環境

図 4 は IoT デバイスを接続した演習環境のイメージを示す．

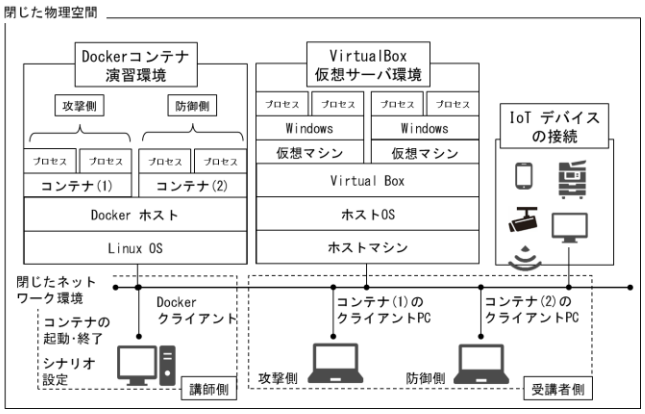

図 4 IoT デバイスを接続した演習イメージ図

IoT に関する攻撃と防御の演習の開発へ拡張する計画である．

3.4 情報倫理とコンプライアンス教育

(1) 教育の必要性

CyExec 演習により得られた技量は，攻撃者視点のものが含まれる．受講者は，故意あるいは過失により，その技術を用いて悪用行為を行う可能性がある．特に社会人経験のない学生は，興味本位でサイバー攻撃を行う側となるリスクが高い．このため，受講者はなにがどのような法律に抵触するか，あるいは倫理的に問題あるかを把握した上で演習に参加する必要がある．

つまり，形式的な誓約書の提出を求めるのみではなく，根本的に何が問題であるか受講者に理解させる必要がある．

(2) 教育カリキュラム案

CyExec 演習に求められる法・倫理教育のカリキュラム案を下記に示す．

(a) セキュリティ事故の事例紹介

加害者の年齢が受講者と近い事例を選択することで，受講者に対し，身近な事例であること理解させる．

(b) セキュリティ関連法律

セキュリティに関連する法律を理解させ，(a) で紹介した事例はどの法律に抵触しているかを解説する．

(c) 情報モラル・情報倫理

セキュリティ分野の技術は進展が早く，技術的対策や法整備が遅れる傾向にある．社会的な規範や慣習に基づ

くモラル，個人の内面的な自律や良心に基づく倫理と，法との関係性を解説する．

（d）責任範囲の確認

受講者に対して責任と自覚を持たせるため，CyExec 演習前に誓約書の提出を求める．

4. CyExec への実装例

前章にて提案した構成を PC 上に実装し，CyExec の演習環境の移植性やプログラムの共同開発の可能性を検証した．

(1) 演習環境の構築

CyExec の演習環境は，VirtualBox を用いて仮想マシンを作成し，ゲスト OS 上に Docker をインストールして構築する． 以下の条件で演習環境を構築した．

- VirtualBox バージョン： 5.1.36
- Docker バージョン： 18.03.0-ce
- ゲスト OS： Ubuntu 16.04.3 LTS
- メモリ： 2GB
- ストレージ： 10GB
- チップセット： PIIX3
- ビデオメモリ： 16MB

(2) 脆弱性診断演習プログラム WebGoat の実装

脆弱性診断演習プログラム WebGoat を，演習環境上の Docker コンテナで動作させる．WebGoat は，実装済みのコンテナイメージが DockerHub に提供されているため，Docker がインストール済みの環境であれば，容易に利用可能である．コンテナイメージをダウンロードし，コンテナを作成・実行することで，ブラウザから Webgoat を実行できることを確認した．

今回の試行で CyExec に実装し稼働を確認したが，WebGoat はテーマ数が多く，解説が不足していることが判明した．教育に使うためには，カリキュラムやテキストなどの開発が必要である．

(3) 演習プログラムの開発と実装

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を開発し，CyExec 上に実装した．

XSS は，入力フォームなど動的な Web ページにおける脆弱性を利用した攻撃方法である．攻撃者は，脆弱性のある Web ページにユーザーを誘導し，不正なスクリプトを実行させる．この環境を実現するため，攻撃者が誘導に使うコンテナと，防御側として脆弱性のある Web ページ動作用のコンテナの 2 つを実装し，受講者に環境を配布する．図 5 は開発した XSS 演習プログラムを実装した環境を示す．

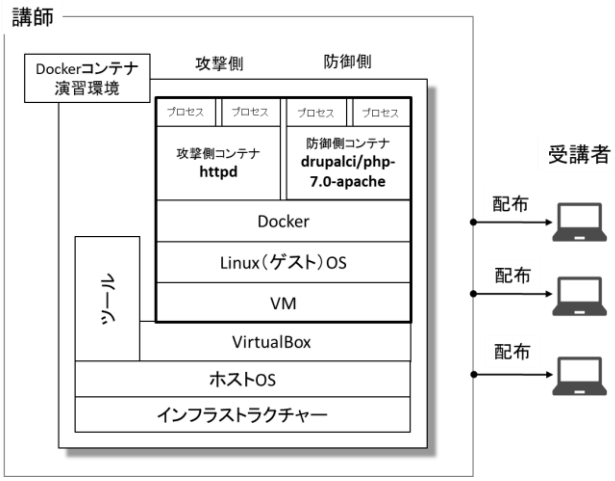

図 5 演習プログラムを実装した環境

脆弱性のある防御側コンテナには，入力フォームの実装とスクリプトの動作のため，PHP が動作する Apache Web サーバコンテナイメージを利用した．

簡単な入力フォームや確認画面等を設置し，氏名や住所などの個人情報の入力を伴う Web ページを作成する．攻撃側は，Web サーバ上に不正なスクリプトを含んだ攻撃用 URL を作成し，脆弱性のある防御側の Web ページへのリンクとして配置する．

受講者は，防御側コンテナの Web ページから，個人情報の登録を行い，動作確認を行う．次に，攻撃側コンテナの Web サーバに設置したリンクから防御側の入力フォームページを開き，正常動作時と同様に登録を行うと，不正なスクリプトによる意図しない動作を確認できる．

実際に攻撃を体験することで，動作の仕組みや，脆弱性に関する知識を学習可能である．また，ソースコード確認による脆弱性箇所の確認，対処法などの学習ができる．

さらに，脆弱性検査の機能を増やすことも可能である．OWASP の提供する ZAP（Zed Attack Proxy）は Web アプリケーションの脆弱性検査を行えるツールであり，DockerHub にコンテナイメージが提供されている[14].

ZAP を用いた演習を追加することで，受講者は実際のツール操作を通して，防御側サーバの脆弱性検査や通信内容の検査などを学習できる．

また，CyExec の演習環境では，自主開発プログラムを実装したコンテナを共有して相互に内容を補うなど，カリキュラムの共同開発を行うことが可能である．複数機関による共同開発，共同利用を促すことで，高等教育機関での導入と演習環境の発展を可能にする．

5. おわりに

サイバー攻撃の増加・高度化に伴い，対応するセキュリティ人材の育成が課題となっている．しかし，人材育成を行う高等教育機関や中小企業では，専用の演習環境の整備，

高額な演習システムの導入，専門知識を持った人材の確保が困難である．このため，教育環境の整備が進まず，セキュリティ人材不足は解決できていない．

本稿では，仮想化技術やオープンソースの演習プログラムを利用し，演習環境の低コスト化と既存人員での運用，演習プログラムの共同開発，共同利用を実現するサイバー攻撃と防御の演習システム CyExec の提案した．

エコシステムの考え方を導入した CyExec では，仮想環境上に実装したコンテナ内で演習プログラムが動作する構成とした．この構成により，複数の教育機関で容易に演習プログラムの開発，追加および利用が可能となる．

現在，CyExec に脆弱性診断演習システム WebGoat の教材開発と攻撃と防御の自主開発プログラムを開発中である．今後は，CyExec を普及させるため，演習プログラムの共同開発，演習環境の共同管理を行うコミュニティの設置を計画している．

謝辞　本研究は，産業技術大学院大学 PBL（Project Based Learning）として実施した．笠井洋輔，夏立娜，黒木大志，長谷川公志，緑川和宏らチームメンバーとの有益な議論に対し，ここに感謝の意を表する．

参考文献

[1] 情報処理推進機構: 情報セキュリティ白書 2017,2017 年 7 月.
[2] 内閣サイバーセキュリティセンター: サイバーセキュリティ戦略,2015 年 9 月 https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf.
[3] 経済産業省: IT 人材の最新動向と将来推計に関する調査結果,2016 年 6 月 http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf.
[4] 情報通信研究機構: 平成 30 年度実践的サイバー防御演習「Cyder」の開催について https://www.nict.go.jp/press/2018/03/07-1.html.
[5] 文部科学省: enPiT 分野・地域を越えた実践的情報教育協働ネットワーク 平成 28 年度成果報告書，2014 年 4 月 http://www.enpit.jp/img_new/publications/enPiT_annualreport_uni_2017.pdf.
[6] 中島滉介ほか: 「攻撃者目線」で学べるシステムセキュリティ実践的学習環境の提案，日本ソフトウェア科学会第 30 回大会，2013 年 9 月.
[7] 江連三香: サイバー攻撃に備えた実践的演習,情報処理 Vol.55 No.7 666-672 ページ,2014 年 7 月.
[8] OWASP WebGoat Project: https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project.
[9] 情報処理推進機構: 脆弱性体験学習ツール AppGoat https://www.ipa.go.jp/security/vuln/appgoat/.
[10]「脆弱性体験学習ツール AppGoat」利用許諾条件合意書　https://www.ipa.go.jp/files/000055105.pdf.
[11] デジタル大辞泉: エコシステム https://kotobank.jp/word/エコシステム-185508.
[12] Oracle VM VirtualBox: http://www.oracle.com/technetwork/jp/server-storage/virtualbox/overview/index.html.
[13] What is Docker: https://www.docker.com/what-docker.
[14] OWASP Zed Attack Proxy Project: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project.
[15] 中田亮太郎ほか: 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，情報処理学会第 80 回大会，2018 年 3 月.
[16] 瀬戸洋一,渡辺慎太郎: サイバーセキュリティ入門講座 DVD 教材,日本工業出版,2018 年.

URL の情報は，2018 年 7 月 9 日時点で確認済み．