様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月 １０ 日現在

機関番号：３２６４４
研究種目：基盤研究(C)（一般）
研究期間：2019～2021
課題番号：１９Ｋ０３００６

研究課題名（和文）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

研究課題名（英文）Proposal of CyExec, an ecosystem-based cyber attack and defense exercise system

研究代表者
慎　祥揆（Shin, Sanggyu）

東海大学・情報理工学部・特任准教授

研究者番号：６０６１５５４０

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：本研究では，教育機関で容易に導入でき，共同開発・共同利用を実現するためのサイバーセキュリティ演習システムCyExec（Cyber security Exercises）の開発を行った．CyExecは，VirtualBoxおよびDockerによる基盤システムと，コンテナによる演習コンテンツから構成される．演習コンテンツは，基礎演習にOWASPのWebGoatを採用し，各種Webアプリケーションの脆弱性診断演習が実施できることを示した．応用演習では，シナリオの例として現実に起こるセキュリティインシデントを再現した実践的なシナリオの開発を通じて，エコシステム（開放環境）としての活用の可能性を示した．

研究成果の学術的意義や社会的意義
CyExecによる演習を実施し，アンケートによる教育効果の検証を行い，高い評価を得ることができ，サイバーセキュリティ演習システムとして一定の効果を確認できた．また，既存の計算機環境で演習を実施でき，コストをかけず容易な導入が可能であることを示した．その上，演習実施の際には演習テキストや補助教材の充実が演習システムの有効性に大きく影響することが確認できた．演習プログラムのエコシステムだけではなく，導入機関同士でテキストや導入ノウハウの積極的な共有を行うことで，より効果的なサイバーセキュリティ人材育成のフレームワークとして活用することができると期待できる．

研究成果の概要（英文）：This study proposed the CyExec (Cyber Security Exercises), a cybersecurity exercise system that educational institutions can quickly introduce to realize joint development and use. CyExec consists of an infrastructure system using VirtualBox and Docker and exercises contents using containers. OWASP's WebGoat was used for the basic exercises, and it was shown that it is possible to perform vulnerability assessment exercises for various web applications. In the application exercises, we developed practical scenarios that reproduce actual security incidents as examples of scenarios to show the possibility of using the system as an ecosystem (open environment).

研究分野：サイバーセキュリティ

キーワード：CyExec　cybersecurity　training platform　cyber range　elearning

１．研究開始当初の背景

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．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・技術不足が懸念されている．

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．しかし，多くの高等教育機関では，演習システムの必要性を認識しつつも，導入コストの高さや演習環境の維持管理を行う人員の不足から，サイバーレンジの導入が進んでいない．

高等教育機関では，演習プログラムや教育カリキュラムの共同開発が可能で，共同利用が容易な演習システムの整備が必要である．

２．研究の目的

サイバーレンジによる演習は，実在するシステムを模して構築した仮想環境上で，現実に起こるインシデントや実際のマルウェアを用いるなど，リアリティの高い効果的な演習が実施できる．しかし，導入コストの高さや演習環境の維持管理の難しいから導入が進んでいない．そのため，サイバーセキュリティ演習システムCyExec（Cyber security Exercise）を開発した．CyExecは，基盤システムと演習コンテンツから構成される．

本研究では，まず（1）攻撃と防御をスタンドアロンで運用する方式（プライットフォーム）を開発する．次に，(2) インターネット環境で攻撃と防御をインタラクティブに対応できるようにする．最終的には，(3) IoT機器を接続し，IoTの攻撃と防御の演習プログラム開発を実現する．これにより，多くの大学で実践的セキュリティ教育が対応可能となると期待できる．

３．研究の方法

CyExecは，高等教育機関や中小企業での導入を想定したサイバー攻撃と防御の基礎技術を学ぶ演習システムである．以下にその特徴を示す．

・低コストで実現する移植性の高い演習環境

演習システム導入・維持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．演習システムの更新には専門的な技術を有する要員が必要で人件費などのコストも大きい．

これらのコストを抑制するには，現有の計算機環境（クライアントPC，サーバー等）で，開発した演習プログラムを容易に実装できる仮想化技術を用いた演習環境を構築する．仮想環境構築にはVirtualBoxを利用する．VirtualBoxは，WindowsやmacOS等（ホストOS）の上に仮想のOS（ゲストOS）を稼働させる．仮想環境上に演習プログラムの動作環境を実装する．

・共同開発・利用が容易な演習環境

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が，セキュリティ分野の技術の進展は早い．このため，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のは困難である．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．このため，エコシステムの考え方を導入し，複数組織での演習プログラムの共同開発・利用を実現する．

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，関連組織全体が発展することを示す言葉である．CyExec は単独の組織だけでなく，関連する組織の共同開発・利用により，CyExecの演習プログラムを充実させる．

複数の高等教育機関による共同開発・利用を実現するためには，異なる機関間でも演習プログラムを容易に開発し利用できる必要がある．Dockerを利用したコンテナ技術にて実現する．

VirtualBoxにて構成した仮想環境上にDockerを実装し，Docker上にコンテナを設置する．脆弱性診断や攻撃や防御に関する様々な演習プログラムを実装してコンテナ上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．また，開発した演習プログラムを稼働させるコンテナのイメージファイルを作成し関連組織内で公開することで共同利用できる．

図1にCyExec演習システムのアーキテクチャを示す．

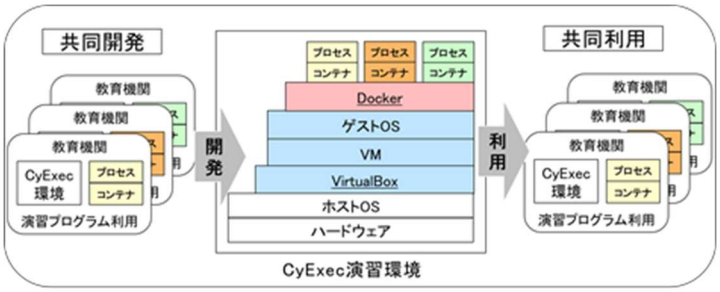

図１　CyExec 演習システムのアーキテクチャ

開発した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，攻撃や防御の演習プログラムが動作するプロセスを Docker 上のコンテナに実装する．VirtualBox のもつ現有計算機環境で動作可能な移植性と Docker コンテナの高い拡張性により，演習プログラムの共同開発・利用を可能とする．

(1) 演習コンテンツ開発

CyExec へ実装する演習コンテンツは,図 2 に示すように基礎演習と応用演習から構成される．

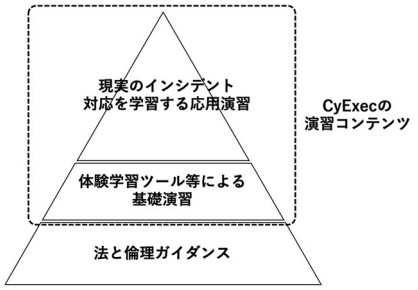

図２　CyExec の演習コンテンツ構成

(2) 基礎演習コンテンツ

基礎演習は，体験学習ツールを用いるなど，脆弱性の概要や検出，対応技術を学習する．応用演習は，実際に起こるインシデントを想定した演習シナリオにより，実践的な知識やスキルを学習する．受講者のレベルや必要な学習内容に対応できる演習シナリオを検討する必要があるが，学習内容の検討には，ITSS+や SecBok が参考となる．ITSS+はセキュリティインシデントに対応する各役割に関し，知識や経験を踏まえたレベルごとに必要なタスクが確認できる．SecBok は，役割ごとに必要となる知識やスキルが具体的に示されている．これらを参考に，必要な学習内容を絞り込んで検討する．

また，CyExec による演習を実施するにあたり，学習した知識やスキルを悪用しないよう，サイバーセキュリティに関係する法律や，事例を交えた法と倫理ガイダンスを実施する．併せて，不正に技術を扱わないなど誓約書へのサインを求める．

(3) 応用演習コンテンツ

応用演習は，実際に起こるインシデントを想定したシナリオに沿って，実践的な知識やスキルを学習する．以下に，応用演習コンテンツとして，Web サーバへの不正アクセスを扱ったシナリオの開発例を示す．演習シナリオは，攻撃側と防御側に分かれる．図 3 に演習シナリオのイメージを示す．

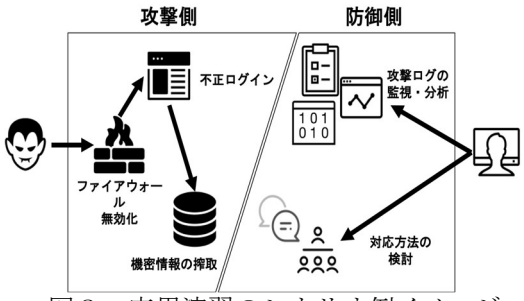

図３　応用演習のシナリオ例イメージ

攻撃側の演習は，攻撃対象のサーバに存在する脆弱性を利用して Web サイトへの不正ログインを行う．ファイルアップロード機能を悪用したバックドアの作成や，データベースへの不正ア

クセスにより，機密情報の窃取を体験する．

４．研究成果

(1) CyExec の基盤システムの構成

提案するサイバーセキュリティ演習システム CyExec は，仮想化技術を用いて現有する計算機環境へ導入して開発した．

ハイパーバイザ型の仮想化は，安定した動作が見込めるが，専用のハードおよびソフトが必要であり，導入コストが高額である．ホスト型の仮想化は，仮想マシンの数が増えると負荷が高くなるが，現有する環境で稼働中のさまざまな OS（ホスト OS）上で利用できるため多くの環境に対応でき，開発した環境の移植も容易である．コンテナ型の仮想化は，他の仮想化方式と比較すると安定性に欠けるが，高速・軽量で高密度な演習環境を構築できる．これらの各仮想化方式の特徴を考慮し，図 1 に示す CyExec アーキテクチャを構成した．

高等教育機関の既存計算機環境上のホスト OS に VirtualBox で仮想マシンを作成し，動作するゲスト OS 上の Docker コンテナで，攻撃や防御の演習プログラムを実装した．これにより，さまざまな教育機関で容易に導入できる移植性の高い演習環境を実現した．

(2) エコシステムとしての活用

演習に用いる攻撃や防御等の動作を再現する各種プログラムは Docker コンテナで実装するが，さまざまなシナリオに対応するプログラムが必要となる．教育機関が単独で開発するのは大きな負担がかかるため，Docker の機能を有効に活用し，エコシステムの考え方による共同開発・共同利用を実現する．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，システムを利用する業界全体が発展することを示す言葉である．

Docker はイメージ共有の機能に優れ，公開されたさまざまなコンテナイメージを開発に利用できる．仮想マシンの場合，用途ごとに OS のインストールや初期設定，サービス立ち上げなど多くの工程が必要だが，Docker は目的に合った機能が実装済みのコンテナが利用でき，多くの工程を短縮できる．そのため，仮想マシンよりも容易かつ短期間での開発が可能である．

(3) 演習課題と演習環境

図４に，WebGoat による SQL Injection の演習課題の例を示す．示す演習課題例は，入力されたユーザの情報をデータベースから取得し，結果を表示する演習プログラムである．このプログラムには SQL インジェクションの脆弱性があり，入力フォームに特定のコードを入力すると，攻撃が成功しユーザ情報の一覧が表示される．

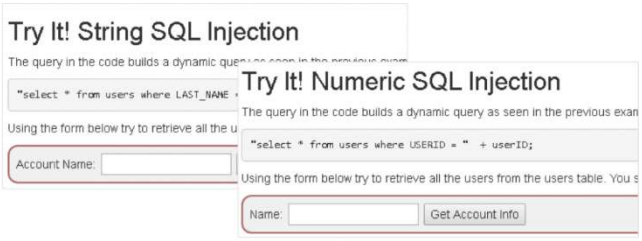

図４　SQL Injection の演習例

攻撃側の演習は，攻撃対象のサーバに存在する脆弱性を利用して Web サイトへの不正ログインを行う．ファイルアップロード機能を悪用したバックドアの作成や，データベースへの不正アクセスにより，機密情報の窃取を体験する．防御側の演習は，ログ分析ツールを用いてアクセスログを調査し，アクセス数やアクセス元，ログイン成否等の情報を可視化する．また，ログイン履歴やアプリケーションログの内容から，攻撃の痕跡を調査する．ログの調査と分析を通じて，対処方法を検討した．実際のシステム環境を考慮し，サーバや利用端末ごとに分けて演習環境を構築する．また，演習実施の際の操作性を考慮し，ホスト OS から仮想環境内の各端末へのアクセスを可能とした．

(4) 基礎演習コンテンツの検証

提案した基礎演習コンテンツの学習効果を検証するため，情報工学系，高専，および社会人大学院修士課程の学生のべ 14 名に対して CyExec による演習を含む授業を実施した．受講対象者はネットワーク，データベース，プログラミング，情報セキュリティ科目の単位を取得済みで，演習の前提となるサイバーセキュリティの基礎知識を有するため，CyExec を用いた演習の学習効果を検証するのに適し，有効な結果を得られると判断した．

設問（図５）は，演習の内容，および模擬授業で使用した教材，講師の説明，TA のサポートに関する内容で構成した．それぞれ 5 段階での評価と，選択した理由の記述により，理解に役立った点や不足した点を確認する内容となっている．図６にアンケートの結果を示す．

演習テーマ	詳細
Q1. 演習問題の理解度	・5 段階評価および理由の記述  理由：
Q2. 演習教材の分かりやすさ	同上
Q3. 講師の説明の分かりやすさ	同上
Q4. TA のサポートの適切さ	同上
Q5. その他，ご意見ご要望	記述：

図５　アンケートの設問内容

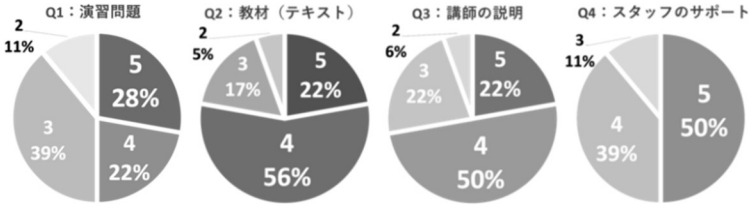

図６　授業後アンケートの結果

すべての設問で，50%以上が 4 以上の高い数値を選択しており，模擬授業の理解度・満足度の高さが示された．特に CyExec の演習効果に直接かかわる Q1 は 5 割が理解できたと回答しており，サイバーセキュリティ教育に効果的であることを確認できた．Q2 および Q3 は，多くの教育機関で汎用的に演習が実施できるよう，日本語テキストや講義用のスライドを準備し，操作方法等も含め，演習経験のない受講者でも円滑に演習が実施できる内容を意識したことで，高い評価を得た．Q4 は，TA は事前に基礎演習の内容を自身で実施し，CyExec 演習環境の実装も行っていたため，演習システムと演習コンテンツどちらの対応も可能であったことで高い評価に繋がった．

(5) IOT セキュリティ演習コンテンツ

IoT 機器も，Web アプリケーションのような脆弱性を有している．これにより，IoT 機器を踏み台とするサイバー攻撃などが増加している．しかし，このような現状について，IoT 機器の開発者や使用者に浸透しておらず，啓発を行う意義は高い．

このため，2 つの応用演習を開発した．一つは IoT カメラ，他はデジタルサイネージに関する演習である．

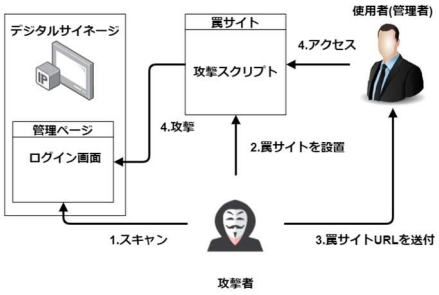

図７　攻撃演習の概要

本演習用プログラムを実装した Raspberry Pi を PC に接続，CyExec を通して操作する．Raspberry Pi の HDMI 端子にディスプレイを接続する．Raspberry Pi とディスプレイは，デジタルサイネージを模している．攻撃者は，CyExec 内のパケット監視ツール OWASP ZAP，テキストエディタ，WebWolf を使用する．使用者(管理者)は，CyExec 内のブラウザを通して Raspberry Pi に実装されたデジタルサイネージを操作する．

(6) AI セキュリティ演習コンテンツ

今回は直接にセキュリティ問題に対するデータを基にした演習コンテンツの開発まではいたらなかったが，公開されている公共データ（人口移動，COVID-19）をもちいたデータ分析研究を学生に対して行った．ある程度の研究成果を出してあったので，今後本システム内に応用し，ダミーのセキュリティ関連のデータを用いた AI セキュリティ演習への拡張可能性を確かめた．

５．主な発表論文等

〔雑誌論文〕　計10件（うち査読付論文　9件／うち国際共著　6件／うちオープンアクセス　9件）

１．著者名 Shin Sanggyu、Seto Yoichi	４．巻 3
２．論文標題 CyExec - Training Platform for Cybersecurity Education Based on a Virtual Environment	５．発行年 2020年
３．雑誌名 International Journal of Learning Technologies and Learning Environments	６．最初と最後の頁 1～20
掲載論文のDOI（デジタルオブジェクト識別子） 10.52731/ijltle.v3.i1.517	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 中田 亮太郎, 慎 祥揆, 笠井 洋輔, 豊田 真一, 瀬戸 洋一	４．巻 11(2)
２．論文標題 エコシステムを実現するサイバーセキュリティ演習システムCyExecの開発	５．発行年 2020年
３．雑誌名 情報処理学会デジタルプラクティス	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Shin Sanggyu、Seto Yoichi	４．巻 -
２．論文標題 Development of IoT Security Exercise Contents for Cyber Security Exercise System	５．発行年 2020年
３．雑誌名 13th International Conference on Human System Interaction HSI 2020	６．最初と最後の頁 281-286
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/HSI49210.2020.9142678	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Shin Sanggyu	４．巻 20
２．論文標題 Introduce the CyExec System for Cybersecurity Training Platform and Cybersecurity Research Trends Related to Data Analysis	５．発行年 2021年
３．雑誌名 東海大学紀要.情報理工学部	６．最初と最後の頁 11-18
掲載論文のDOI（デジタルオブジェクト識別子） 10.18995/24352152.20.11	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Nobuaki Maki, Ryotaro Nakata, Shinichi Toyoda, Yosuke Kasai, Sanggyu Shin, and Yoichi Seto	4．巻 10(3)
2．論文標題 An Effective Cybersecurity Exercises Platform CyExec and its Training Contents	5．発行年 2020年
3．雑誌名 International Journal of Information and Education Technology	6．最初と最後の頁 215-221
掲載論文のDOI（デジタルオブジェクト識別子） 10.18178/ijiet.2020.10.3.1366	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Sanggyu Shin, Yoichi Seto, Yosuke Kasai, Rituna Ka, Daishi Kuroki, Shinichi Toyoda, Koji Hasegawa, Kazuhiro Midorikawa	4．巻 1
2．論文標題 Development of Training System and Practice Contents for Cybersecurity Education	5．発行年 2019年
3．雑誌名 2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI)	6．最初と最後の頁 172-177
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/IIAI-AAI.2019.00043	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Kato Zen、Shin Sanggyu	4．巻 -
2．論文標題 Economic Impact Analysis of News Articles Based on Polarity Analysis of News : Impact research of COVID-19 using market data	5．発行年 2021年
3．雑誌名 14th International Conference on Human System Interaction (HSI)	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/hsi52170.2021.9538749	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Shimizu Shuto、Shin Sanggyu	4．巻 -
2．論文標題 Applicability of SARIMA Model in Tokyo Population Migration Forecast	5．発行年 2021年
3．雑誌名 14th International Conference on Human System Interaction (HSI)	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/hsi52170.2021.9538690	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 瀬戸 洋一，中田 亮太郎	４．巻 13
２．論文標題 コンテナ型仮想化技術を利用したサイバーセキュリティ攻撃と防御演習システムCyExecの開発	５．発行年 2019年
３．雑誌名 産業技術大学院大学紀要	６．最初と最後の頁 47-54
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 瀬戸 洋一，牧 宣彰	４．巻 13
２．論文標題 サイバー攻撃と防御演習コンテンツWebwolfno高等教育への利用可能性の検討	５．発行年 2019年
３．雑誌名 産業技術大学院大学紀要	６．最初と最後の頁 115-119
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 渡辺 嶺，石川 大輔，駒野 勝己，盛 宸，畑谷 成郎，牧 宣彰，慎　祥揆，瀬戸 洋一
２．発表標題 IoTセキュリティ演習コンテンツの開発とサイバーセキュリティ演習システムCyExecへの実装
３．学会等名 電子情報通信学会　情報セキュリティ研究専門委員会　（ISEC研）
４．発表年 2020年

１．発表者名 牧 宣彰，畑谷 成郎，駒野 勝己，渡辺 嶺，盛 宸，石川 大輔，慎　祥揆，瀬戸 洋一
２．発表標題 WebWolf演習コンテンツの調査分析
３．学会等名 情報処理学会コンピュータセキュリティ研究会，　セキュリティ心理学とトラスト研究会
４．発表年 2019年

１．発表者名
石川 大輔，渡辺　嶺，駒野 勝己，盛　宸，畑谷 成郎，牧　宣彰，慎　祥揆，瀬戸 洋一

２．発表標題
サイバーセキュリティ演習システムCyExecへのIoTセキュリティ演習コンテンツの開発

３．学会等名
情報処理学会第82回全国大会

４．発表年
2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

私立大学情報教育協会（JUCE）は，全国の私立大学向けに毎年セキュリティに関する講習会を実施しており，その中でサイバーレンジシステムCyExec を使ったインシデント対応演習を実施した（2019年）．
演習は，会場となった大学のコンピュータ演習室の環境を借りて実施した．実施前日にネットブートシステムのマスタイメージを作成し，演習環境を全てのPCに配布して起動した．
CyExec のサンプルシナリオとして用意されている「Web サーバへの不正アクセス」を用いて，攻撃の実施から防御の一連の流れを，ペアワークも交えて体験することで，インシデント対応方法を学習した．仮想インスタンス（コンテナ）が6 つの，比較的多くのネットワーク構成を再現した環境である．CyExec はコンテナを使うことで移植性が高く軽量な実行環境を実現しており，前日からの準備でも滞りなく快適な演習環境を提供することができた．演習の受講者は，全国の私立大学の情報部門の担当者や関係する教員など，約30 名である．（JUCE Journal 2019年度 No.4，pp.55）

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	瀬戸　洋一 (Seto Yoichi) (50417036)	東京都立産業技術大学院大学・産業技術研究科・名誉教授 (22605)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関