デジタルプラクティス　Vol.11 No.2(Apr. 2020)

一般投稿論文

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

中田 亮太郎[1,2]　慎 祥揆[3]　笠井 洋輔[1]　豊田 真一[1]　瀬戸 洋一[1]

[1]産業技術大学院大学　[2]情報セキュリティ大学院大学　[3]東海大学

サイバー攻撃の脅威が拡大し，攻撃手法の高度化が進んでいる．一方，対応するセキュリティ人材の不足が深刻化している．セキュリティ人材育成に効果的な市販の演習システムは，コストおよび運用における課題があり，高等教育機関での導入は進んでいない．セキュリティ人材の育成は喫緊の課題となっている．したがって，高等教育機関への演習システムの整備は急務である．このため，オープンソースソフトウェアを利用して構成するサイバーセキュリティ演習システムCyExec（Cyber security Exercises）を開発した．導入が容易で，共同開発・共同利用が可能なエコシステムとしての利用を特徴とし，教育機関での柔軟な演習内容の変更が可能である．本稿では，CyExec演習システムの開発，および教育機関における有効性の検証結果ついて述べる．

1. はじめに

サイバー攻撃によるセキュリティインシデントの発生件数が増加している．2018年1月の仮想通貨流出事件や，2019年7月のコンビニ決済サービス不正利用事件など，事業継続や社会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．2020年には19万人以上の人材が不足する見込みであり，すでにセキュリティ業務に従事する人材の専門知識や技術の不足も懸念されている[2],[3]．

セキュリティ人材育成の取り組みとして，一部の高等教育機関では実践的な演習形式の教育が行われている．専用の体験学習ツールによる演習や，実際のセキュリティインシデントを想定した訓練ができるサイバーレンジによる演習がある[4],[5]．

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，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[5],[6]．

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．

© 2020 Information Processing Society of Japan

基盤システムは，VirtualBoxやDockerなど，オープンソースソフトウェアを用いることで低コストで導入・維持が可能である．また，高い移植性を持つアーキテクチャにより，多くの組織で容易に導入が可能である．導入組織間で演習プログラムをエコシステムとして共同開発・共同利用することで開発の負担を減らし，多様なカリキュラムへの対応が可能である．

演習コンテンツは，基礎と応用に分け構成される．基礎編として体験学習ツールの実装，応用編として攻撃と防御のインタラクティブなシナリオを開発し，演習プログラムを実装した[5],[6],[7].

本稿では，第2章でサイバーセキュリティ教育の状況と課題，第3章でサイバーセキュリティ演習システムCyExecの提案，第4章でCyExecへ実装する演習コンテンツの内容，第5章でCyExecを用いた演習による教育効果の検証について述べる．

2. サイバーセキュリティ教育の現状と課題

2.1 サイバーセキュリティ教育の状況

表1に，実践的なサイバーセキュリティ教育を実施している高等教育機関の状況を示す[5].

表1 高等教育機関でのサイバーセキュリティ教育の取り組み状況

大学	内容	教員体制	備考
東京工業大学	在籍する学生を対象に，「サイバーセキュリティ特別専門学修プログラム」として，2016年度から5つの講座を開講	概論科目は学内教員が担当，その他は協力企業の外部講師が担当	野村総研，楽天，NTT，産総研の協力でカリキュラム作成，講座の実施
東京電機大学	CISOや上級エンジニアを目指す社会人や大学院生向けに，国際化サイバーセキュリティ学特別コース「CySec」を開講	学内教員と企業等の外部講師によるオムニバス形式で実施	攻撃技術，フォレンジック，心理，法と倫理と，幅広いカリキュラム設定
情報セキュリティ大学院大学	在籍する学生を対象とした実習科目として，3つの講座が設けられている．企業からの支援によりサイバーレンジを導入し，大学院側との協業体制により演習を実施	学内教員と企業等の外部講師によるオムニバス形式で実施	
enPiT関係	基礎科目・演習・先進科目から構成される．大学院生向けに開講されているが，学部生向けのコースも設置し，11大学で連携．社会人向けコースは，実践技術を学びキャリアパス構築を支援する講座を7大学で実施	一部の大学では，講義は学内教員と企業等の外部講師によるオムニバス形式で実施	5つの大学（情セ大，奈良先端大，北陸先端大，東北大，慶應大）を中心に実施

これらの教育機関では，講義形式のみではなく演習形式の授業を実施している．実践力を伴った人材を育成するカリキュラムを設定し，その維持のため企業や外部組織との連携，専門家の支援を受けた運用体制をとっている．

© 2020 Information Processing Society of Japan

上記に紹介した以外にセキュリティ教育を実施している高等教育機関の多くは，暗号やネットワークを専門とする教員により，情報セキュリティの概論あるいは暗号技術の教育の実施にとどまっている．

サイバーセキュリティ教育は単独でカリキュラム開発や演習を実施するには負担が大きく，費用面・人材面で企業等の支援を受けずにカリキュラムを維持することが難しい．多くの教育機関は，実践的サイバーセキュリティ教育の必要性を感じているが，対処できていないのが現状である．

2.2　サイバーセキュリティ演習の課題

実践的なサイバーセキュリティ教育を行っている教育機関で採用している演習方式として，体験学習ツールによる演習とサイバーレンジによる演習がある．**表2**に演習の概要と課題を示す．

表2　サイバーセキュリティ演習の概要と課題

	体験学習ツール	サイバーレンジ
目的	・攻撃手法の体験 ・脆弱性の検出および対策技術の習得	・攻撃と防御技術の習得 ・役割に応じた実践的な対応
対象	・システムやアプリケーションの脆弱性（主にWebアプリケーション	・セキュリティ機器，ネットワーク機器およびシステム，サービスなど全域 ・インシデントに対応する各役割における担当者
代表例	・WebGoat（OWASP） ・AppGoat（IPA）	・CYBERIUM（富士通） ・TAME Range（IAI） ・ADI Cyber Range（ADI）
特徴	・低コストで演習環境を構築可能 ・Webアプリを中心とした脆弱性検出と対策	・サイバー攻撃や防御の相互演習 ・組織的な対応方法の習得 ・実際のマルウェアや現実におこるインシデントを再現
費用	・無償	・数千万～数億の導入費用 ・機器保守費用 ・シナリオ開発費用 ・演習実施や維持の人件費・委託費
課題	・演習シナリオが固定 ・一部を除き攻撃と防御の相互演習が未整備 ・組織的な対応方法は学習範囲外	・導入，維持管理コストが高額 ・演習シナリオの自由な変更や追加が困難 ・演習実施や環境維持に専門知識を持つ人員が必要

体験学習ツールによる演習は，PCに脆弱性の概要や診断，および対策などを体験し，知識や技術を習得する．代表例として，セキュアなソフトウェア開発を促進するコミュニティであるOWASP（Open Web Application Security Project）が提供するWebGoatや，IPA（情報処理推進機構）が提供するAppGoatがある．

AppGoatは，集合教育を想定したカリキュラムが策定されているが，カリキュラム変更が困難なため柔軟性に欠ける．また，ツールの改訂が定期的に行われていないため，新しい脆弱性への対応が遅くなる[8]．WebGoatは，技術変化に合わせたプログラムの改訂作業が随時実施されているが，学習素材のみの提供であり，演習実施には別途カリキュラムやテキストの整備が必要である．また，完成度が不十分な演習も含まれ，利用にあたっては事前の分析が必要である[9]．

© 2020 Information Processing Society of Japan

それぞれ無償で公開されており，利用時はPCにインストールして演習環境を構築する．低コストで演習環境を構築できるが，演習シナリオは固定されており，組織的なインシデント対応手法は学習範囲外である．また，学習範囲は脆弱性の検出および対策に限定され，攻撃側と防御側に分かれたインタラクティブな演習に欠ける．

サイバーレンジによる演習は，CSIRT（Computer Security Incident Response Team）やSOC（Security Operation Center）など，セキュリティインシデントに対応可能な組織的人材の育成を目的とした実践的演習である．サイバーレンジで構築する演習環境は，専用に用意した機器で動作する仮想環境にクライアント，サーバ，ネットワークなど現実のシステム環境を模して構築する[5]．

さまざまな攻撃手法やマルウェアへの対応，被害状況の確認や脆弱性への対応方法の訓練など，攻撃発生から対応終結までの一連の流れを想定した学習が可能だが，サイバーレンジは導入・維持コストが非常に高額である．また，市販の製品は導入組織の意向に合わせたシナリオ変更の柔軟性に欠け，演習実施や維持管理に専門の知識を持つ人員が必要となる．

これらの演習では実践的な知識の習得が可能であり，特に社会経験の少ない学生が容易に実世界で攻撃を実施してしまうなど，悪用のリスクに対する教育も必要となる．

以上のように，サイバーセキュリティの演習はコスト面や対応人材，演習シナリオ，および安全面に関する課題がある．これらの課題に対応するため，次章で述べるサイバーセキュリティ演習システムCyExecを開発した[6],[7]．

3. サイバーセキュリティ演習システムCyExecの提案

3.1 サイバーセキュリティ演習の課題への対策

2.2節で述べたサイバーセキュリティ演習の課題への対策として，**表3**に示す特徴を持つ演習システムを検討した．

表3　新サイバーセキュリティ演習システムの特徴

課題	対策や考慮点	特徴
コスト	仮想化技術を活用し，現有計算機環境で演習環境を構築	OSSの利用により，導入・維持コストの負担を最小限に抑え，容易な導入を可能とする．
対応人材	企業や専門家の協力無しでも，教育機関の既存の教員構成で演習を実施	基礎演習コンテンツとしてOSSベースの体験学習ツールを利用することで，最新の脆弱性に対応する．また，演習用テキストや資料を充実させ，演習の実施を容易にする．
シナリオ	複数の教育機関による共同開発・共同利用可能なシステム	共同開発・共同利用が容易なエコシステムとして公開し，単独での開発負担を軽減する．コンテンツの充実やノウハウの共有でサイバーセキュリティ教育環境全体を発展させる．
安全面	知識や技術の不正利用を防止する教育	演習前の誓約や，法と倫理教育の実施を必須とし，適正なコンプライアンス知識を身に着けた上で演習を実施する．

© 2020 Information Processing Society of Japan

これらの特徴を満たし，高等教育機関で積極的に導入・利用が可能な仕組みとして，以下の内容を提案する．

（1）演習システム

市販の演習システムを導入維持するには，高等教育機関では経費負担が大きい．また，受講する学生の能力に合わせた演習内容の調整が必要であるが，カスタマイズが容易ではない．このため，仮想化技術を用いて，教育機関で所有するサーバやPCなど既存の計算機環境を利用して導入可能な演習システムとする．OSS（オープンソースソフトウェア）を用いることで低コストな導入・運用を実現し，演習実施のための高い移植性とカスタマイズ性を持つシステムとして構成する．演習システム構成の詳細については次節以降で説明する．

（2）演習コンテンツ

演習での学習内容やシナリオは，教育目的や受講者の能力などを考慮した開発が必要である．このため，脅威や脆弱性などを学習する基礎演習と，より実践的に攻撃と防御の技術を学習する応用演習に分け，段階的に学習する仕組みとする．

基礎演習は，サイバーセキュリティ教育に必要な基礎知識を，OSSベースの体験学習ツールを利用して学習する．たとえばWebGoatは，毎年新たな脆弱性に関する改訂がされており，最新の脆弱性に対応できるメリットがある．応用演習は，実際のシステム環境を想定し，現実に起こるセキュリティインシデントを想定した実践的な対応手法を学習する．演習シナリオに応じた攻撃や防御の演習プログラムや，演習用テキストの開発が必要となる．演習コンテンツについての詳細は第4章で説明する．

また，受講者が演習を通じて得たスキルが，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り，演習実施の際には事前指導を行う．

3.2　サイバーセキュリティ演習システム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する．利用する仮想化方式は，**表4**に示す3つを比較し検討した．

表4　仮想化方式の比較

方式	特徴	メリット	デメリット
ハイパーバイザ型	専用ハードウェア上でハイパーバイザと呼ばれるプログラムが動作し，仮想マシンを構築	仮想マシンが他からの影響を受けにくく，安定している	専用機器や有償ソフトが必要で，導入コストが高い
ホスト型	稼働中のOS上に導入する専用ソフトがハイパーバイザの役割を担い，仮想マシンを構築	既存の環境で使えるため，容易に導入可能	オーバーヘッド（遅延）が他に比べ大きくなりがち
コンテナ型	OS上で必要なプロセスを分離させ，仮想マシンとして動作させる	余計なプロセスが無く，高速・軽量に動作	ホストOSや他コンテナの影響が大きい

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，

© 2020 Information Processing Society of Japan

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．

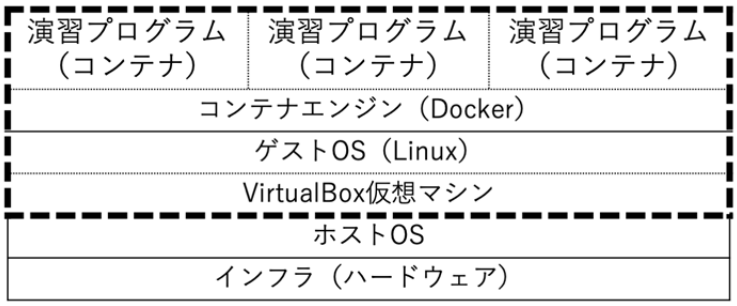

図1　CyExecのアーキテクチャ

ホスト型仮想化とコンテナ型仮想化を組み合わせて利用したCyExecアーキテクチャの特徴を以下に示す．

（1）現有する計算機環境に依存しない演習環境

多くの教育機関で利用するため，現有する計算機環境の状況に依存せず導入可能なシステムとする．そのため，ホスト型の仮想化ソフトウェアであるVirtualBoxを基盤システムとして採用した．VirtualBoxで作られた仮想マシンは，エクスポート・インポートの機能により容易に別の環境へ移植して利用することができる．また，対応するOSが多く，多くの教育機関で現有する計算機環境に導入することができる．

（2）高い移植性を持つ演習環境

演習の実施にはさまざまな攻撃や防御のプログラムが必要となる．そのため，コンテナ型の仮想化ソフトウェアであるDockerを用いて演習プログラムを実装する．Dockerは必要なプロセスのみをホストOSからグループ化して分離させて動作するため，余分なプロセスが動作せず効率よくリソースを活用できる．そのため，VirtualBoxで構築した仮想マシン上に多くのコンテナを動作させても，高い移植性を損ねることがない．

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する．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する．

3.3　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[6]．

© 2020 Information Processing Society of Japan

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．また，開発したコンテナイメージを教育機関で共有することで，エコシステム体制を確保する．**図2**に，CyExecの共同利用イメージを示す．

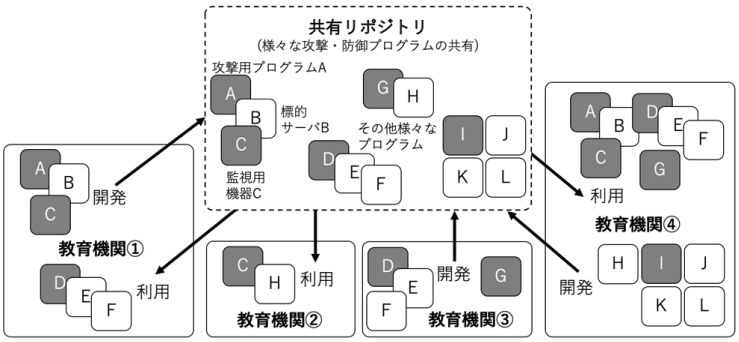

図2　エコシステムとしてのCyExec利用イメージ

教育機関ごとに開発した演習用プログラムを共有し，他の教育機関でも利用可能とする．開発元の教育機関でも，他で開発したプログラムを利用することで開発の負担軽減やコンテンツの充実を図ることができる．公式に用意されているDockerHUBのような公開されたリポジトリでは悪用のリスクがあるが，Dockerのプライベートリポジトリの機能により，制限された範囲でのコンテナイメージ共有が可能であるため，CyExec導入機関での共同開発・共同利用体制を容易に構築することができる．

4. 演習コンテンツ

4.1 演習コンテンツの基本構成

CyExecへ実装する演習コンテンツは，**図3**に示すように基礎演習と応用演習から構成される．

© 2020 Information Processing Society of Japan

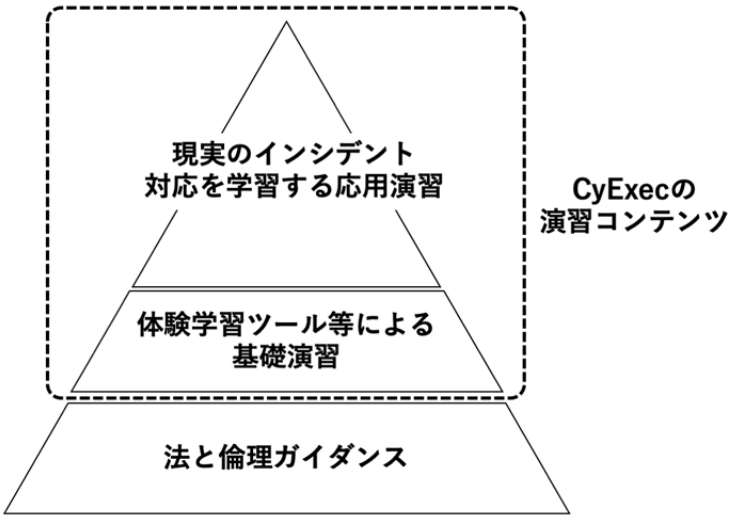

図3　CyExecの演習コンテンツ構成

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[10]．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[11]．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[7]．

次節以降で，演習コンテンツの内容について例を示す．

4.2　WebGoatによる基礎演習

体験学習ツールWebGoatは，脆弱性の概要と検出，および対策方法を体験し学習できる．内容も定期的に更新されており，必要な内容を選択して演習に利用できるため，基礎演習コンテンツとして適している．

表5にWebGoatの演習テーマの概要を示す[9]．

© 2020 Information Processing Society of Japan

表5　WebGOATの取り扱いテーマ概要

演習テーマ	詳細
Introduction	WebGoatの概要
	WebWolfの概要
General	HTTPベーシック
	HTTPプロキシ
Injection Flaws	SQLインジェクション（上級）
	SQLインジェクション
	SQLインジェクション（初級）
	XXE(XML External Entity)
Authentication Flaws	認証の回避
	JSON Webトークン（JWT）
	パスワードリセット
Cross-site Scripting	クロスサイトスクリプティング（XSS）
Access Control Flaws	安全でないオブジェクトの参照
	アクセス制御機能の欠陥
Insecure Communication	安全でないログイン
Insecure Deserialazation	安全でないデシリアライゼーション
Request Forgeries	クロスサイトリクエストフォージェリ
Vulnerable Components	脆弱なコンポーネントの利用
Client Side	フロントエンドの制限回避
	クライアント側のフィルタリング
	HTMLの改ざん
Challenges	Webgoat総合演習

WebGoatによる基礎演習の内容に関し，SQLインジェクションを例に説明する．SQLインジェクションはWebGoatで扱われているコンテンツの中でも特に被害が多い攻撃手法の1つで，攻撃体験を通じた高い学習効果が期待できる．

（1）演習目的

SQLの基礎知識とSQLインジェクションの脆弱性の概要，検出方法について演習課題を通じて理解し，サイバー攻撃と防御の基礎技術を修得する．

（2）修得可能なスキル（SecBokより該当する項目を抜粋）

- 脆弱性診断に関する基礎知識
- 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攻撃の認知とカテゴライズに関するスキル

（3）攻撃手法の例

SQLインジェクションは，入力データの一部がリテラル（SQL文中の定数）をはみ出し，SQL文の内容が変わることが主な原因である．**図4**にSQLインジェクションの攻撃例を示す．

© 2020 Information Processing Society of Japan

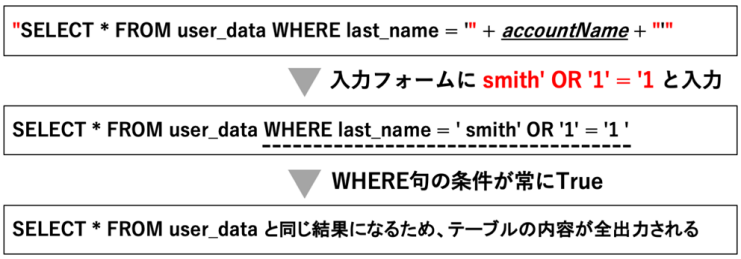

図4　SQLインジェクションの攻撃例

last_nameを検索条件としてuser_dataテーブルを検索するSQL文で，accountNameは入力フォームから受け取った値を格納する変数である．ここに特定の文字列を送信することで，WHERE句の条件が必ず真となり，すべてのデータを検索対象としてしまう．

このように，SQLインジェクションの脆弱性がある実装は，入力値によりSQL文が改変され，意図しない実行結果を発生させる可能性がある．

（4）演習課題

図5に，WebGoatによるSQL Injectionの演習課題の例を示す．

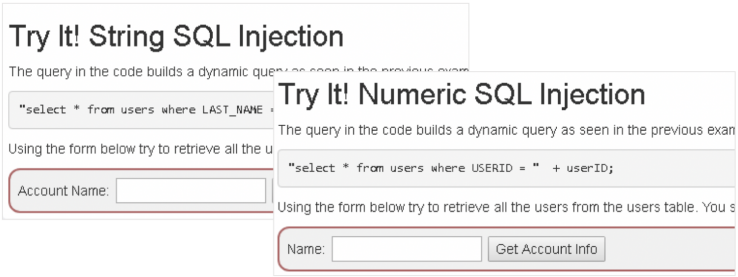

図5　SQL Injectionの演習例

演習課題は，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．

（5）CyExecを用いた演習への活用

WebGoatは，javaを用いたスタンドアロン版の他，Dockerコンテナによるインストール手順が公開されている．演習で利用する際は，個別インストールによる手間やバージョン・設定など細かな違いが発生しないよう，CyExec上に実装したイメージを移植する．これにより，教育機関の既存計算機環境や，受講者自身のPC等に容易に統一した環境が準備できる．

© 2020 Information Processing Society of Japan

また，WebGoatは，（3）で示した演習課題のような学習素材のみの提供であり，演習を実施するには，カリキュラムの作成と演習内容を解説するテキストの整備が必要である．さらに，導入手順や講師用ガイダンスを準備し共有することで，低コストで容易な導入が可能な演習システムとして活用が可能である．

4.3　応用演習コンテンツの開発例

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．

（1）演習目的

組織内での各役割ごとの対応力向上のため，システム管理者，攻撃者，利用者など複数の視点で演習を実施することにより，セキュリティインシデントへの対応手法を総合的に習得する．

（2）習得可能なスキル（SecBokより該当する項目を抜粋）

- セキュリティシステムにおける脆弱性スキャンの実施と脆弱性の認識に関するスキル
- ペネトレーションテストの原理，ツールおよび技術に関する知識
- サーバ診断ツールと障害識別技法に関する知識

（3）演習シナリオ

演習シナリオは，攻撃側と防御側に分かれる．**図6**に演習シナリオのイメージを示す．

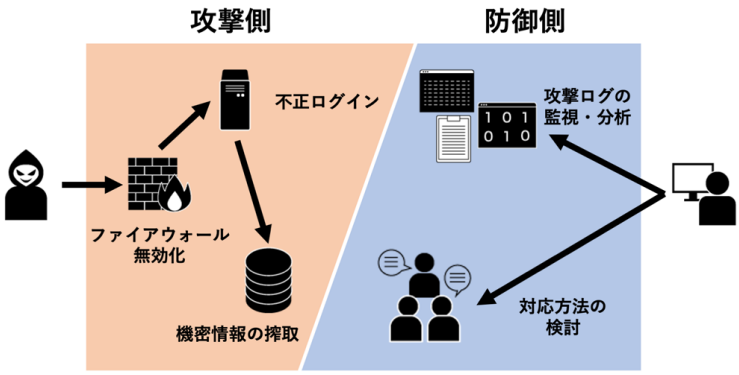

図6　応用演習のシナリオ例イメージ

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[12],[13]．

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，対処方法を検討する[14]．

（4）仮想ネットワーク構成

© 2020 Information Processing Society of Japan

図7に演習環境の仮想ネットワーク構成を示す．

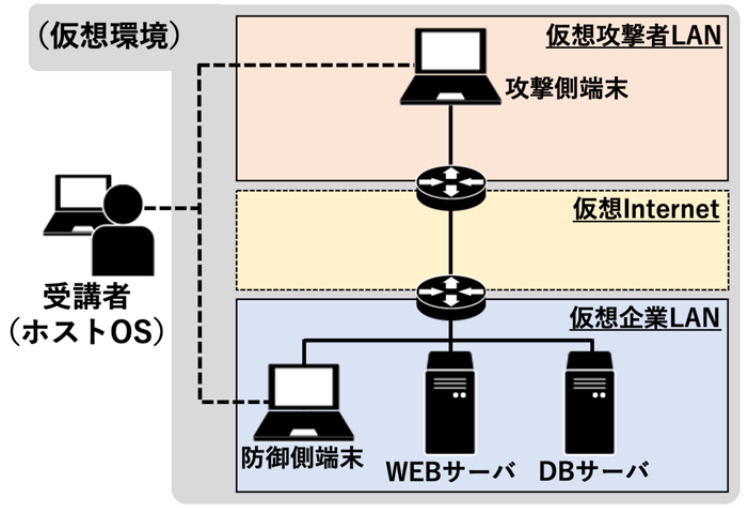

図7　応用演習のネットワーク構成例

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する．

図8にCyExecに実装した演習プログラムの構成を示す．

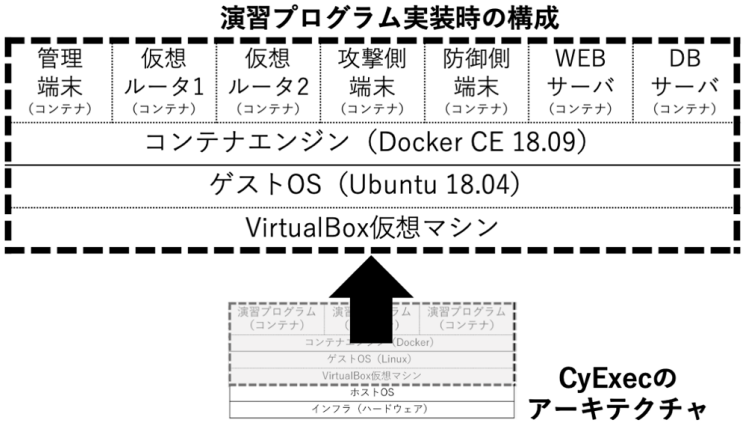

図8　実装した演習プログラムのコンテナ構成

Dockerコンテナにより，演習シナリオの再現に必要な仮想ルータ，操作用のデスクトップ端末，サーバなどを実装し，必要なネットワーク設定を行う．

（5）システム要件

表6に開発した応用演習環境のシステム要件を示す．

© 2020 Information Processing Society of Japan

表6　応用演習環境のシステム要件

ゲスト OS	OS	Ubuntu 18.04
	メモリ	2GB
	ストレージ	20GB
	コンテナ構築	Docker CE 18.09
演習プログラム	プログラム言語	Ruby 2.5.1, PHP 7.2
	データベース	Mysql 8.0
	Web サーバ	Apache 2.4

ゲストOS内で仮想的に多くの端末が操作する高密度な環境を構築するが，コンテナを使用することでゲストOSやホスト機への負荷を最小限に抑えられる．

（6）開発

応用演習の開発は，演習シナリオを作成し，その環境を再現する演習プログラムの開発と実装を行う．**図9**に開発の流れを示す．

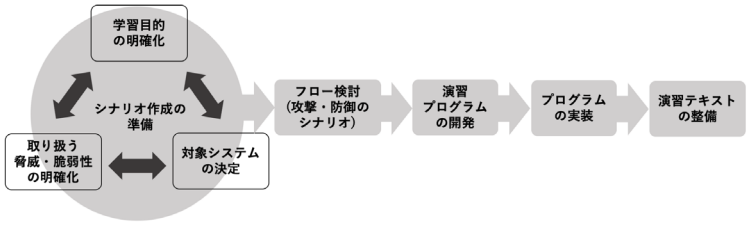

図9　応用演習の開発手順

演習シナリオは，学習対象とするスキルの内容や取り扱う脆弱性を明確化し，それらを実現可能なシステムを対象とすることで検討を行う．最新のSecBokスキル項目やOWASP Top 10の脆弱性を参考にするなど，具体的なシステム環境や使用するツールを含め検討することで，実践的な演習シナリオが作成できる．

演習プログラムの開発にはDockerHubを利用し，WebサーバやDBサーバなど，目的の機能が実装済みのコンテナの利用や，Ubuntuが動作するコンテナで操作端末や仮想ルータを開発することで，作業負担を大幅に軽減できる．また，Dockerのプライベートリポジトリ機能で，複数の開発環境で演習プログラムを共有することで，容易に共同開発の環境を整えられる．エコシステムとして他の教育機関等と共同利用・共同開発を行う場合も，同様の方法で実現する．

また，演習の際に受講者が参考とするため，使用するツールの解説やシナリオの遂行に必要な知識等を解説した補助資料を作成する．必要に応じて講師用のガイダンス資料を用意するなど，演習を円滑に実施するための各種テキストの整備を行う．

5. CyExecの活用と学習効果の検証

5.1　基礎演習コンテンツの検証

© 2020 Information Processing Society of Japan

4.2節に示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．

CyExecの開発に関与した産業技術大学院大学の学生が講師やTA（Teaching Assistant）を担当して授業をサポートし，演習内容は，Injection Flaws（SQL Injection）とAuthentication Flaws（Authentication Bypasses）を使用した．時間が限られていたため，事前にCyExecおよび基礎演習コンテンツを実装した演習用PCを用意した．また，円滑に演習を行うため，日本語訳のテキストを用意し，演習で必要となるスキルについての解説を講義形式で実施した後，演習を行った．

表7に，授業後に実施したアンケートの設問内容を示す．

表7　アンケートの設問内容

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 1　3　5 理解できなかった　普通　十分理解した 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：

設問は，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10**にアンケートの結果を示す．

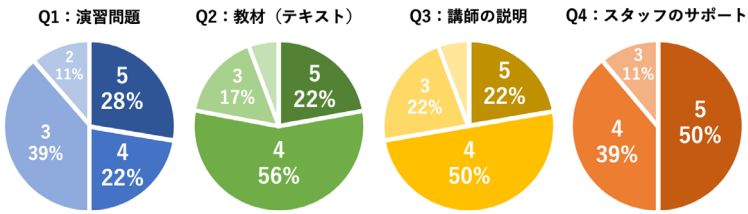

図10　授業後アンケートの結果

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

© 2020 Information Processing Society of Japan

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．

自由記述への回答内容を以下に示す．

（1）ポジティブな意見

- 授業内容が理解しやすく，日本語演習教材の活用などにより理解が促進された
- サイバーセキュリティに対する興味が強まった
- 具体的な脆弱性検出などシンプルな内容で分かりやすく，演習がスムーズに進んだ
- 手間どった演習も詳細な説明やTAのサポートより回答できた

回答の内容から，演習による理解の促進が確認できた．また，演習がスムーズに実施できたことや，講師による適切な解説や補助教材の充実に関する評価も得た．特に，日本語によるテキストを用いた講師の説明やTAのサポートに関する意見が多く見られ，補助教材や演習のサポート体制の重要性も確認できた．

（2）ネガティブな意見

- 演習課題を回答するためには前提知識が必要であるため，事前に詳細な説明が必要である
- 抽象的な話ではなく事例など具体的な内容の説明がほしい
- 3時間の模擬授業では時間が少なく，演習解説の説明が理解できない部分があった

回答の内容から，演習により理解が促進できることが確認できた．また，演習がスムーズに実施できたことや，講師による適切な解説や補助教材の充実に関する評価も得た．特に，日本語によるテキストを用いた講師の説明やTAのサポートに関する意見も見られ，補助教材や演習のサポート体制の重要性が確認できた．ただし，演習の難易度や時間設定に関する課題を確認した．さらなる教材の改善や，講師用ガイダンスの充実により，演習による効果がより高くなるよう開発を進める．

5.2　応用演習コンテンツの検証

4.2節で示した応用演習コンテンツを用いた演習を，高等教育機関の教職員を対象とした講習会で実施した．参加者は21大学23名で，情報システム部門の職員を中心に，他部門職員や教員も参加した．受講対象者は，セキュリティインシデント発生の際に各所属組織の技術的対応の中心となる立場であり，応用演習の学習効果を検証するのに適する．また，システムの選定や導入にかかわる立場でもあるため，CyExecが自組織の環境で演習に活用できるかなど，普及や共同利用に関する評価を得ることも可能である．

演習に対応した人員は講師1名と，産業技術大学院大学の学生3名，および講習会の運営スタッフ2名がサポートを行った．2日間の情報セキュリティに関する講習会の1セッションとしてCyExecを用いた演習を実施し，アンケート調査による検証を行った．**表8**に演習の詳細を示す．

© 2020 Information Processing Society of Japan

表8　演習環境および実施内容の詳細

内容	詳細	備考
実施環境	教卓 PC 1 台 受講者用 PC 50 台を準備	ネットブートシステムを利用した一斉展開
演習用 PC	OS:Windows8.1 CPU:Intel Core-i5 Memory:8GB Strage:120GB 割り当て	ネットブート用の雛形イメージに，VirtualBox のみ追加インストール
CyExec	CyExec 基盤イメージ及びシナリオ用イメージを使用	VirtualBox へ CyExec 環境インポート及びシナリオ実装
演習環境 事前準備	雛形機作成・検証	事前日程を確保し約 1 時間
	雛形機展開・受講者用 PC 動作確認	展開に約 30 分，動作確認に約 30 分
	ホスト機起動・ CyExec 環境準備	当日の演習準備．6 名で約 30 台を約 30 分で完了
資料・ テキスト	事前学習資料	サイバーレンジの概要，取り扱う脆弱性，使用するツール等の解説，用語集等
	演習用テキスト	CyExec シナリオ開発時のものを活用し作成
	コマンドリスト	演習内で使用するコマンドの一覧
演習内容	応用演習サンプルシナリオ Web サーバへの不正アクセス	休憩や解説を挟み、約 3 時間の演習を実施
	インシデント報告演習	演習の内容を報告書にまとめ，CISO への報告を想定したペアワークを 1 時間実施
アンケート	CyExec 演習に対する WEB アンケート	演習に関する 10 の設問と自由記述による回答

演習は高等教育機関の教室を借り，既存の計算機環境を利用して実施した．環境を事前に準備するため，雛形機にVirtualBoxのインストールとCyExecの基盤環境，および応用演習コンテンツを実装し，ネットブートシステムによる一斉展開後，起動やシナリオの遂行に問題がないことを確認した．実施当日は，ホスト機の起動から演習環境準備までをスタッフで実施した．

システム以外の準備として，演習用テキストの他，事前配布資料を作成し，予備知識の習得を促した．また，操作に不慣れな受講者が遅れないよう，演習内で使用するコマンドをあらかじめリスト化したものを用意し，参考にできるよう配布した．演習実施後にアンケートによる検証を実施した．**表9**にアンケートの内容を示す．

表9　応用演習のアンケート項目

設問	回答
Q1.目的・目標が示されていた	0～10 の 11 段階評価
Q2.難易度は適切であった	同上
Q3.学習量が適切であった	同上
Q4.学習範囲は適切であった	同上
Q5.目標を達成できる内容であった	同上
Q6.説明は簡潔でわかりやすかった	同上
Q7.講師の話は適切であった	同上
Q8.演習の時間管理は適切であった	同上
Q9.教材は内容理解に役立った	同上
Q10.周囲の方々へも受講を勧めたい	同上
その他	自由記述

© 2020 Information Processing Society of Japan

演習の効果を検証するための内容や教材に関する設問の他，CyExecの普及や継続利用の可能性を確認するため，マーケティングで用いられる手法であるNPS（Net Promoter Score）の算出方法を参考にし，周囲へ勧める可能性を問う設問を含めた11段階の評価と自由記述への回答を求め，21名から回答を得た[15].

図11にアンケートの結果を示す.

	0	1	2	3	4	5	6	7	8	9	10	平均
Q1	0	0	0	0	0	0	0	1	2	0	18	**9.7**
Q2	0	0	0	3	0	1	0	0	4	4	11	**8.9**
Q3	0	0	0	0	0	2	1	0	7	2	9	**8.6**
Q4	0	0	0	0	0	2	1	0	2	8	8	**8.8**
Q5	0	0	0	0	1	0	0	1	4	2	13	**9.1**
Q6	0	0	0	0	0	0	0	1	5	1	14	**9.3**
Q7	0	0	0	0	0	0	0	1	1	1	18	**9.7**
Q8	0	0	0	0	0	0	0	1	2	0	18	**9.7**
Q9	0	0	0	0	0	0	0	1	1	5	14	**9.5**
Q10	0	0	0	0	1	0	0	1	5	0	14	**9.1**

図11　応用演習アンケートの結果

全体で非常に高い評価を得た．4.3節で示したように，演習コンテンツの目的やスキルを明確にすることで，受講者は目的意識を持ち演習に臨むことができ，Q1やQ5の高い評価に繋がった．Q2～Q4による難易度や学習範囲に関する設問では，受講者の知識やスキルにより評価が分かれる可能性が考えられたが，事前学習資料で必要な知識を補えたことや，コマンドリストにより操作スキルの差を埋められたことで，スキルの低い受講者でも安心して受講でき，高い評価に繋がった．ただし，一部のスキルの高い受講者には簡単な内容となり，待機時間も発生していたため，今後はグループ学習による役割ごとの変化のある対応や，追加要素で詳細な調査を行うなど，より充実したコンテンツ開発を進める.

講師は筆者が務めたが，それ以外のスタッフはCyExecの開発に直接かかわってはいない．ただし，シナリオを事前に確認したことや，資料・テキストを充実させたことでサポートの負担も大幅に軽減され，演習の進行も滞りなく実行でき，Q6～Q9の進行面や教材の高い評価に繋がった.

また，Q10の設問を元に求めたNPS（回答ごとに，9・10を推奨者，7・8を中立者，6以下を批判者とし，推奨者-批判者の割合で算出）は61.9と高いスコアを示した．サンプルの少なさや，比較データがないことから，今後さらに多くの検証は必要となるが，CyExecの利用や広く普及させることへのポジティブな評価として参考になった.

自由記述への回答内容を以下に示す.

- 実際の攻撃とその痕跡を見ることができ，大変参考になった.
- 実践的で臨場感があり，特に攻撃側の体験は貴重で効果があったと思う．防御側の演習ももっと体験してみたい.
- ツールと基本的なコマンドだけで情報漏えいに繋がる可能性があることに恐怖を覚えた.
- 講師の進行が分かりやすく，トピックの入れ方も良かった.
- セキュリティ人材育成での演習システムの重要性を感じた.

© 2020 Information Processing Society of Japan

- 演習を部署のメンバにも体験してもらい，スキルアップや意識の向上にも役立てたい．

実際のシステムを模した環境で攻撃や防御を体験する臨場感が伝わり，実践的な演習が実施できた．演習システム対する評価も高く，CyExecのサイバーセキュリティ演習システムとしての有効性を確認できた．さらに，テキストを充実させることで円滑な進行が可能となり，効果的で満足度の高い演習が実施できた．

6. おわりに

サイバーセキュリティ人材の育成に用いられる演習システムは，コストの高さや運用面などの課題から，高等教育機関での導入が進んでいない，このため，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の開発を行った．

CyExecは，VirtualBoxおよびDockerエンジン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．VirtualBoxによる仮想マシンの高い移植性と，Dockerコンテナによる演習コンテンツをエコシステムとして活用が可能なアーキテクチャが特徴である．演習コンテンツの共同開発・共同利用を進めることで，単独での開発の負担を軽減し，さまざまな教育機関の多様なカリキュラムへ対応できる．

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．応用演習は，シナリオの一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，開発手法やDockerコンテナによるエコシステムとしての活用の可能性を示した．

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った結果，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．また，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．

CyExecは，2019年7月の時点で1つの企業，6つの大学，3つの専門学校へ移管済である．今後，移管先の組織でも検証を行い，演習コンテンツの充実と演習効果の向上を図る．

謝辞　本研究は，産業技術大学院大学のProject Based Learning（PBL）教育の一環で開発した．関係したPBLメンバに謝意を表する．本研究はJSPS科研費JP16K 19K03006の助成を受けた．

参考文献

1）情報処理推進機構：情報セキュリティ白書2018,
https://www.ipa.go.jp/files/000070313.pdf (2018).
2）内閣サイバーセキュリティセンタ：サイバーセキュリティ戦略,
https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf (2019年8月1日現在)
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,
http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf (2019年8月1日現在)

© 2020 Information Processing Society of Japan

4）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, pp.666-672 (2014).
5）中田亮太郎，長谷川久美，瀬戸洋一：コンテナ型仮想化技術によるサイバー攻撃と防御の演習システムCyExecの開発，情報処理学会第80回全国大会講演論文集2018 (1), pp.415-416 (2018).
6）豊田真一，中田亮太郎，長谷川久美，慎　祥揆，瀬戸洋一：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，Computer Security Simposium2018 (2018).
7）笠井洋輔，夏　立娜，黒木大志，豊田真一，長谷川公志，緑川和宏，慎　祥揆，瀬戸洋一：サイバーセキュリティ演習システムCyExecを用いた演習コンテンツの開発，2019年 暗号と情報セキュリティシンポジウム (2019).
8）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/ (2019年8月1日現在)
9）OWASP：OWASP WebGoat Project, https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project (2019年8月1日現在)
10）情報処理推進機構（IPA）：ITSS+（プラス）・ITスキル標準（ITSS）・情報システムユーザスキル標準（UISS）関連情報，https://www.ipa.go.jp/jinzai/itss/itssplus.html (2019年8月1日現在)
11）日本ネットワークセキュリティ協会（JNSA）：セキュリティ知識分野（SecBok2019），https://www.jnsa.org/result/2018/skillmap/ (2019年8月1日現在)
12）徳丸　浩：体系的に学ぶ 安全なWebアプリケーションの作り方 第2版 脆弱性が生まれる原理と対策の実践，SB Creative (2018).
13）IPUSIRON：ハッキング・ラボのつくりかた 仮想環境におけるハッカー体験学習，翔泳社 (2018).
14）八木　毅，青木一史，秋山満昭，幾世知範，高田雄太，千葉大紀，実践サイバーセキュリティモニタリング，コロナ社 (2016).
15）Reicheld, F.：The Ultimate Question 2.0 (Revised and Expanded Edition)：How Net Promoter Companies Thrive in a Customer Driven World, Harvard Business Review Press (2011).

中田 亮太郎（学生会員）dgs184101@iisec.ac.jp
2018年産業技術大学院大学修士課程修了（情報アーキテクチャ専攻），同年情報セキュリティ大学院大学情報セキュリティ研究科博士後期課程入学（在学中）．昭和女子大学にて従事し，情報セキュリティの研究や人材育成活動を行う．JASA情報セキュリティ内部監査人．私立大学情報教育協会情報セキュリティ講習会運営委員．私立大学キャンパスシステム研究会システム運用管理分科会運営委員．情報システム学修士（専門職）．

慎 祥揆（正会員）shin.sanggyu.t@tokai.ac.jp
2009年慶應義塾大学大学院工学研究科開放環境科学専攻後期博士課程単位取得後退学．2010年から2011年まで慶應義塾大学理工学部准訪問研究員歴任．2011年から2019年まで，産業技術大学院大学　助教．2019年より東海大学コンピュータ応用工学科特任准教授．データマイニング，プライバシー保護，情報セキュリティに関する教育研究に従事．工学博士（慶大）．

豊田 真一（非会員）a1625st@aiit.ac.jp

© 2020 Information Processing Society of Japan

2019年産業技術大学院大学修士課程修了（情報アーキテクチャ専攻）．情報システム学修士（専門職）．アプリケーション開発者，自治体職員，団体職員を経験．主に情報化推進および情報セキュリティ担当として従事．基幹業務のITシステム企画や組織内における情報セキュリティ施策，および個人情報保護に関する研修を実施．

笠井 洋輔（非会員）a1708yk@aiit.ac.jp
2019年産業技術大学院大学修士課程修了（情報アーキテクチャ専攻）．情報システム学修士（専門職）．2014年よりITエンジニア．主に業務用Webアプリケーションの開発業務に従事．2018年にNTTデータイントラマートに入社し，システム共通基盤として利用するパッケージソフトウェアの開発に携わる．Oracle認定Javaプログラマ．JASA情報セキュリティ内部監査人．

瀬戸 洋一（正会員）seto.yoichi@aiit.ac.jp
1979年慶応義塾大学大学院修士課程修了（電気工学専攻），同年日立製作所入社，システム開発研究所にて，画像処理，情報セキュリティの研究に従事．2006年より現在まで，産業技術大学院大学教授．情報セキュリティ，プライバシーリスク評価技術の教育研究に従事．工学博士（慶大），技術士（情報工学），情報処理安全確保支援士．2010年経済産業省産業技術環境局長賞など受賞，著書『実践的プライバシーリスク評価技法』等．

投稿受付：2019年8月19日
採録決定：2020年1月6日
編集担当：串田高幸（日本アイ・ビー・エム（株））

© 2020 Information Processing Society of Japan