体験型サイバーセキュリティ学習システムの提案と再評価

八代 哲[1]　田邉 一寿[1]　齋藤 祐太[1]　齋藤 孝道[2]

概要：本論文では，サイバーセキュリティの専門スキルを養成するため，体験型の演習システムを提案する．提案するシステムでの演習は，セキュリティの初学者が受講することを想定し，限られた時間でのスキルの習得を狙って設計した．受講者は，標的型攻撃，及び，SQL インジェクション攻撃を主な題材としたストーリー型の演習を通して，インシデントレスポンスに必要な基礎的な技術的スキルを学習できる．また，提案システムはクラウド上に構築されているので，演習を行う時間や地理的な制約がなく，受講者の数に応じて提案システムのスケーリングもできる．2018 年 5 月までに，中高生，大学生及び社会人約 300 名が提案システムを用いた演習を受講した．本論文では，提案システムの拡張の詳細と，提案システム全体の評価について示す．

A Proposal and Re-evaluation of Hands-on Learning System for Cybersecurity

SATOSHI YASHIRO[1]　KAZUHISA TANABE[1]　YUTA SAITO[1]　TAKAMICHI SAITO[2]

1. はじめに

経済産業省の調査 [1] によると，企業におけるサイバーセキュリティの専門人材が，2020 年に約 19.3 万人不足するとされている．サイバーセキュリティ人材の育成が社会から求められている背景もあり，主に，インシデントレスポンスの能力の育成を目的として，体験型の演習が様々行われている [2] [3]．それらの体験型演習では実務に近い学習ができる一方，受講者にセキュリティに関する前提知識や，非技術的な業務の経験を求めることも少なくない．また，多くの体験型演習においては，演習のためのシステム環境を用意する必要があることや，高度な専門性だけでなく，教育経験を十分に有するインストラクターを必要とすることもあり，演習の開催の機会も限定される．さらに，多くの体験型演習においては，システム環境の制約もあり，1 度に演習を受けられる受講者の数に限りがある．

以上のことを課題と考え，それらを解決すべく，我々の研究グループでは，サイバーセキュリティに関するテクニカルスキルの習得を目的とし，仮想空間上でのシステム操作を通して学習するシステム（以降，提案システムと呼ぶ）を構築し，その学習効果の部分的な評価を行った [4]．

演習の題材として，標的型攻撃と SQL インジェクション攻撃の 2 つを主に扱っており，それらの題材を扱うストーリー型の演習を通し，インシデントレスポンスの全体像，及びインシデントレスポンスに必要な知識や技術を習得することを狙う．

提案システムは，Windows や Linux の端末等のシステム操作を行う演習環境と，ドキュメント教材や確認テスト機能を提供する学習支援システムの 2 つで構成されている．受講者は，まず，演習に必要な知識の獲得を学習支援システムで行う．その上で，その知識を使って，演習環境上でのログの参照・検索などの操作等を行う．実際に演習内容を十分に理解できたのかを確認するため，学習支援システムにて，操作の演習後に確認テストを行う．また，学習支援システムでは，受講者の操作の手順が示されており，確認テストの採点は自動化されているので，受講者は，インストラクターの支援がなくても自習が可能である．

提案システムはクラウド上に構築されているので，受講者は場所や時間を選ばずに，提案システムを用いた演習を行うことが可能である．また，演習環境は複製することが可能なので，受講者の増加にも対応することができる．

[1] 明治大学大学院
Graduate School of Meiji University
[2] 明治大学
Meiji University

本論文では，文献 [4] からの変更点を含めて提案システムの詳細や，提案システムを用いた演習の評価について示す．

2. 関連知識

本節では，提案システムに関連する攻撃及び用語について説明する．

提案システムの演習では，標的型攻撃及びその対処や，SQL インジェクション攻撃及びその対策を含む，EC サイトからの情報流出事件の全体像 [5] を学ぶことができる．

2.1 標的型攻撃

標的型攻撃とは，組織における機密情報の窃取等を目的とした攻撃の一つである [6]．主に，標的型メール，水飲み場サイト，及び，USB 等の可搬式ストレージを契機としていることが知られている．その中でもメールを契機とした，標的型メール攻撃の報告件数が増加している [7]．

IPA の報告 [8] によると，組織に大きな影響を及ぼしたセキュリティ上の脅威として「標的型攻撃による情報流出」が第 1 位であることから，標的型攻撃は危険度の高い攻撃であると言える．しかしながら，IPA の別の報告 [9] によると，標的型攻撃自体，及びその脅威を知らないと答えた回答者は全体の 48.1%であった．

このことから，標的型メール攻撃の被害が増加している原因の一つに，標的型攻撃の認知度が低いことが挙げられる．

よって，一般的な IT 利用者及び IT システム運用者においては，標的型攻撃自体とその脅威について理解することが重要である．

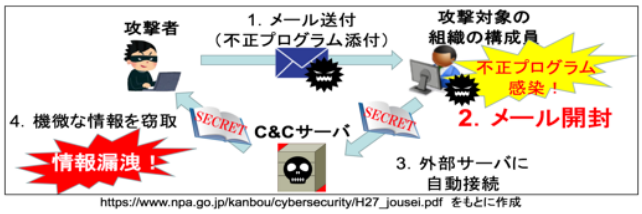

図 1 標的型攻撃の概要

2.2 SQL インジェクション攻撃

SQL インジェクション攻撃とは，Web アプリケーション，及び，Web アプリケーションと連携するデータベースに，攻撃者が不正な操作をすることで，データベースの機密情報等が流出する可能性のある攻撃である．この攻撃は，Web アプリケーションの内部において SQL 文の組み立て方法に問題がある場合に発生する [10]．

文献 [8] によると，組織に大きな影響を及ぼしたセキュリティ上の脅威として，「Web サービスからの個人情報の窃取」が第 3 位となっている．この攻撃の根本的な対策として，SQL インジェクション脆弱性を作り込まない実装を実現することが挙げられている．

よって，Web アプリケーション開発者，及び，IT システム運用者においては，SQL インジェクション攻撃の概念とその脅威について理解することが重要である．

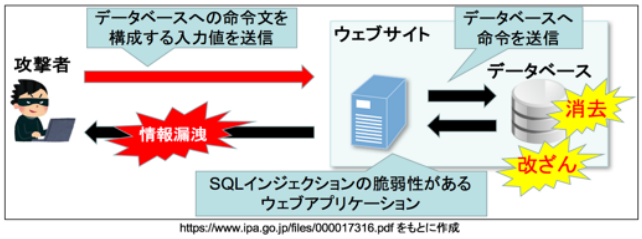

図 2 SQL インジェクションの概要

2.3 インシデントレスポンス

インシデントレスポンスとは，情報流出，改ざん，及び，DDoS 攻撃等のセキュリティインシデントが発生した際に，その被害を最小限にするための対応のことである [11]．

インシデントレスポンスには，インシデントが発生する前の準備段階から，インシデント発生後の対応を含む，いくつかのフェーズがある．文献 [12] に基づき，図 3 にインシデントレスポンスのライフサイクルを示し，各フェーズの概要を以下に示す．

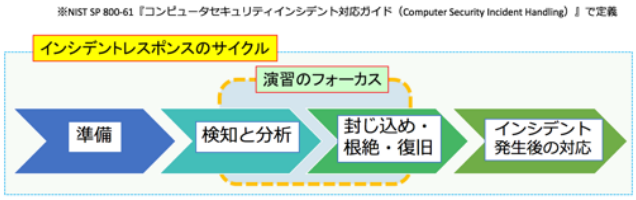

図 3 インシデントレスポンスのサイクル

- 準備
  インシデントが発生した際に必要となる分析用のツール等の準備したり，システム，ネットワーク及びアプリケーションを安全な状態に保ち，インシデントを予防したりするフェーズである
- 検知と分析
  インシデントが発生したかどうかを検知し，もし発生したのであればインシデントの種類，影響の範囲，被害の規模を正確に判断するフェーズである
- 封じ込め・根絶・復旧
  インシデントの封じ込め，証拠の収集，インシデントが発生した原因の除去及びシステムを通常の運用状態に復旧させることを行うフェーズである
- インシデント発生後の対応
  一連のインシデントレスポンスの流れや発生したインシデントについて振り返り，インシデントの対策の有

効性等をレビューするフェーズである

演習は，図 3 における，「検知と分析」及び「封じ込め・根絶・復旧」の技術対応に焦点を当てて構成されている．それらに該当する技術的なスキルを身につけることを目的の一つとしている．

3. 提案システム

ここでは，提案システムについて，システムの構成，運用，利用について説明する．

3.1 提案システムの概要

提案システムは，演習を行うための仮想的なネットワークであるサイバーレンジ（以降，C/R と呼ぶ）と，演習を支援する学習支援システムから構成される．提案システムの全体像を図 4 に示す．

一般に C/R とは，サイバー空間上で行われる演習及びその演習環境のことを指すが，本論文では，クラウド上の複数の仮想マシンで構成された演習環境のことを C/R と呼ぶ [13]．

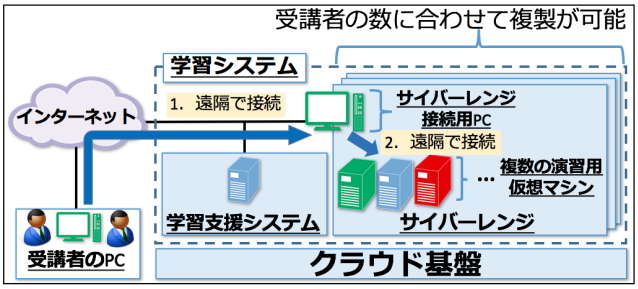

図 4 提案システムの概要図

提案システムにおいて，1 セットの C/R は 13 台の仮想マシンで構成されており，実際のネットワーク環境を模している．演習は 2 人 1 組で行うことを前提としており，1 組で 1 セットの C/R を占有的に利用する．同時に複数の受講者の組が演習を行う場合は，提案システムの管理者がクラウド上で C/R を複製する．

学習支援システムは，演習の進め方，各仮想マシンへのアクセス方法，演習で扱う知識問題等，演習に必要なあらゆる情報を受講者に提供する．

提案システムでは，閉じた仮想空間である C/R 上で仮想マシンの操作を行うので，サイバー攻撃の攻撃者としての演習も可能である．標的型攻撃については，遠隔操作マルウエアの操作等が可能であり，SQL インジェクション攻撃については，C/R 上に用意された独自の EC サイトへの操作等が可能である．

3.2 提案システムの利用概要

受講者は，学習支援システムの操作方法等の情報をもとに，C/R で，実際に PC や Linux の操作をしながら演習する．前述の通り，提案システムに置ける演習は 2 人 1 組で行うことを前提としており，1 組で 1 セットの C/R を占有的に利用する．

次に，受講者が演習を開始するまでの流れを以下に示す．

(1) 受講者は，ブラウザを用いて学習支援システムに接続する．学習支援システムには，サイバーレンジ接続用 PC への接続方法が示されている
(2) 受講者は，サイバーレンジ接続用 PC に接続する
(3) 受講者は，学習支援システム上で演習の進め方や，C/R の使用方法を学ぶ
(4) 受講者は，サイバーレンジ接続用 PC から C/R 内の各仮想マシンに接続し，演習を行う

3.3 C/R

1 セットの C/R は，13 台の仮想マシンで構成されている．C/R の各仮想マシン名と対応する OS 名を表 1 に示す．また，C/R 内のネットワーク構成を図 5 に示す．

表 1 各仮想マシンと OS の対応表

仮想マシン名	OS 名
社内 PC	Windows，Ubuntu 16.04
フォレンジック PC サイバーレンジ接続用 PC	Windows
Active Directory	Windows Server
Web サーバ	CentOS 6.7
DNS サーバ プロキシサーバ 攻撃者のサーバ その他のサーバ	Ubuntu 16.04

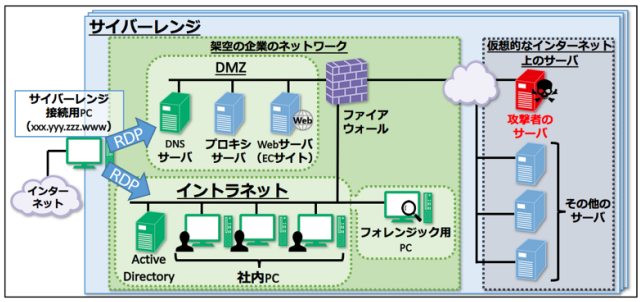

図 5 C/R のネットワーク構成図

図 5 のサイバーレンジ接続用 PC は，インターネットと C/R の仮想的なネットワークとの境界に置かれ，C/R 内の他の仮想マシンに接続するための踏み台となる仮想マシンである．受講者は，サイバーレンジ接続用 PC に接続し，C/R 内の各仮想マシンを操作する．なお，サイバーレンジ接続用 PC へのアクセスは，RDP（Remote Desktop Protocol）接続にて行う．受講者は，インターネットが利用できる環境があれば，場所を選ばずに C/R を用いて演

習を行うことができる．

サイバーレンジ接続用 PC から，C/R 内の各仮想マシンへの接続も同様に，RDP 接続で行う．

図 5 の各仮想マシンの概要を以下に示す（図中の xxx.yyy.zzz.www はグローバル IP アドレスを表す）．

- DNS サーバ
  演習のための架空の企業における社内向けの DNS サーバ．演習のため，脆弱性が作り込まれている Web アプリケーションも動作している．受講者はこのサーバへの脆弱性スキャンの演習を行う
- プロキシサーバ
  社内 PC から仮想的なインターネットへの接続を中継するプロキシサーバ．プロキシサーバを経由した通信のアクセスログをすべて取っている
- Web サーバ
  架空の企業で運用している EC サイト．演習のために，あらかじめ SQL インジェクション脆弱性が作り込まれている
- Active Directory
  社内 PC を管理しているサーバ．演習のために，Active Directory の監査ログを出力する設定となっている
- 社内 PC
  架空の企業の一般社員が使用しているという設定の PC
- フォレンジック PC
  フォレンジック用のツールがあらかじめ準備されている PC である．受講者は，メモリやディスクの解析をこの PC 上で行う
- 攻撃者のサーバ
  架空の企業のネットワーク内に侵入し，攻撃を実施する攻撃者のサーバ

3.4 学習支援システム

学習支援システムは，Moodle [14] により実現する．Moodle とは，オープンソースの e ラーニングプラットフォームであり，ブラウザを用いて接続できる Web アプリケーションである．受講者は，学習支援システムから提示されるスライドを見ることで，演習内容の概要及び演習を行う上で必要な知識を学習することができる．

提案システムでの演習は初学者が対象であるので，詳細な演習の手順はスライドで提示することで，初学者でもスムーズに演習を進められるようにした．特に，RDP 接続の方法等の，演習をする上で必須の操作や，サイバー演習をする上で必要な知識は，学習支援システムで提供することとした．

演習を進めながら，学習支援システム内で出題される確認テストに受講者が解答をすると，自動で採点される．

以上により，インストラクターが不在でも演習が成立するように工夫した．

図 6 学習支援システムログイン後の画面

3.5 演習の概要

前述の通り，演習の題材は大きく分けて 2 つある．1 つ目は標的型攻撃を学ぶ演習（以降，標的型攻撃編と呼ぶ）であり，2 つ目は SQL インジェクション攻撃を学ぶ演習（以降，SQL インジェクション編と呼ぶ）である．演習の詳細は，次節で示す．

受講者は，架空の EC サイトを運営している企業の情報システム部員の立場で，ストーリー課題による演習を行う．また，一つの演習あたり最大 10 時間程度の演習時間を想定している．

各編の演習の流れを図 7 に示し，以下でその説明をする．いずれの演習も「前提知識の学習」，「実践トレーニング」及び「振り返り学習」の順番で構成される．

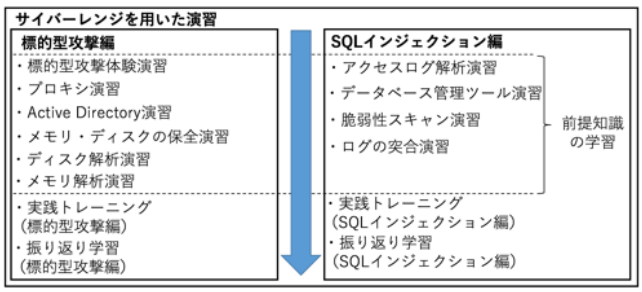

図 7 演習の項目と進め方

(1) 前提知識の学習

受講者は，演習を行う上で必要な基礎的な知識やツールの使い方を学習する．また，学習支援システム上に準備されているスライドを見ることで演習の概要や，演習で使用するコマンドの使い方等を学習する．その後，学習した知識を応用して C/R を操作することで確認テストに解答する．各編に前提知識の学習が 4〜6 項目あり（図 7 参照），標的型攻撃体験演習とメモリ・ディスクの保全演習以外の各項目に確認テストがある．すべての確認テストに正答すると，受講者は実

践トレーニングに進むことができる．内容は，主に，インシデントレスポンスであるが，後の実践トレーニング演習に関係する攻撃の演習も行うことができる．この演習では，この後の演習で必要な知識，すなわち，インシデントレスポンスに必須の技術の習得を狙っている．

図 8　前提知識の学習・確認テスト例

(2) 実践トレーニング

前提知識の学習後，ストーリー型の演習を行う．この演習は，架空の企業が標的型攻撃もしくは SQL インジェクション攻撃を受けている疑いがあると，社外の組織から通知された場面から開始する．これらのストーリーは，実際に発生した攻撃事例に基づいて作成された．受講者は，C/R に準備されている各仮想マシンから出力されたログや，ディスク及びメモリのダンプ等を解析することで，攻撃の特定，被害状況について調査する．また，その対処も行う．実践トレーニングにおいても確認テストがある．すべての確認テストに正答すると，受講者は振り返り学習に進むことができる．

この演習では，実際のストーリーに近い形で，個別の解析方法を有機的に適用する能力を養うことを狙っている．

(3) 振り返り学習

実践トレーニングにおいて扱った攻撃が発生してから，攻撃が終了するまでの流れを振り返る学習である．受講者は，学習支援システム上で確認テストに解答しながら，図 9 に示すような図を作成することで，攻撃の一連の流れを復習することができる．

この演習では，攻撃全体の流れを確認する演習であり，攻撃の個別の事象を時系列に並べる能力を養うことを狙っている．

3.6　演習内容の詳細

各編の目的と，演習の目的と学習項目について示す．

3.6.1　標的型攻撃編

本演習では，C/R 上に擬似的に用意された標的型攻撃の対応及び標的型攻撃を体験する演習を通して，標的型攻撃の理解，対応手順及びインシデント対応に必要な準備の概要を，ネットワーク運用者の観点で習得する．また，簡易的なフォレンジック等のインシデントレスポンスの俯瞰をして，インシデントレスポンスの運用を設計する能力を養う．

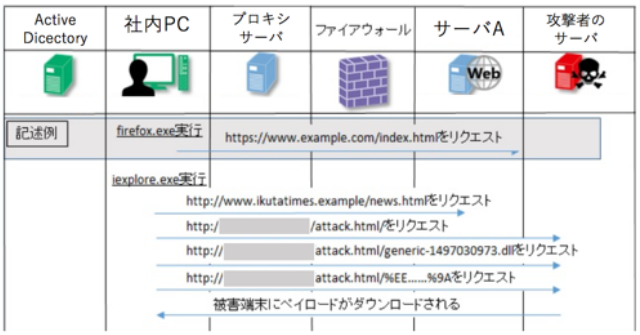

図 9　振り返り学習

次に，標的型攻撃編における学習項目を表 2 に示す．

表 2　標的型攻撃編の学習項目

学習項目
プロキシ，Active Directory のログの見方及び検索方法
HDD，メモリの保全操作及び簡易フォレンジック
Metasploit[15] を用いた，CVE-2015-0311[16] 及び MS11-003[17] を悪用した攻撃演習
遠隔操作型マルウエアによる悪性通信の解析
遠隔操作型マルウエアが HDD 及びメモリに残す情報の解析

3.6.2　SQL インジェクション編

本演習では，C/R 上に擬似的に用意された EC サイトへの攻撃の分析及び暫定対処の演習を通して，EC サイトへの攻撃の理解，対応手順及びそのために必要な準備の概要を EC サイト運用者及び構築者の観点で習得する．

本演習では，SQL インジェクション攻撃及び逆ブルートフォース攻撃を題材としている．また，Web ペネトレーションテストや DBMS の操作等の関連技術の俯瞰をして，インシデントレスポンスの運用を設計する能力を養う．

次に，SQL インジェクション攻撃編における学習項目を表 3 に示す．

表 3　SQL インジェクション編の学習項目

学習項目
ツールを用いた MySQL サーバの操作及びログの検索方法
ツールを用いた Web サーバのログ解析
脆弱性スキャンツールを用いた，Web アプリケーションへのペネトレーションテスト
SQL インジェクション攻撃により残ったログの解析，攻撃者の特定，脆弱なコードの特定及び簡単なセキュアプログラミング
複数のログの突合

4.　演習の題材として追加した攻撃と関連演習

本論文にて，新たに追加した演習の内容について説明する．

4.1 Web サーバに対する攻撃のログ解析演習

本演習は，Web サーバソフトウェアの一つである Apache HTTP Server（以降，Apache と呼ぶ）に対する DoS/DDoS 攻撃のログを受講者が解析し，発生した攻撃の詳細を特定する演習である．

演習で解析するログは，あらかじめ脆弱性を悪用した攻撃を C/R 内で発生させることで，C/R 内に準備した．

演習の際は，受講者はログが置かれている仮想マシンに接続し，less コマンドや grep コマンド等を利用してログの解析を行う．

本演習では，以下の 3 種類の脆弱性を悪用した DoS/DDoS 攻撃のログを解析することができる．

- CVE-2011-3192
  Apache バージョン 1.3 系及び 2.x 系に含まれている，Range ヘッダ及び Request-Range ヘッダの処理に起因する DoS 攻撃に対する脆弱性．この脆弱性を悪用した攻撃のツールとして Apache Killer[18] がある．
- CVE-2014-6271
  GNU Bash4.3 系以前の一部のバージョンに含まれている，環境変数の処理の問題に起因する任意の OS コマンドを実行される脆弱性．この脆弱性は，Shellshock 脆弱性として広く知られている [19]．
- CVE-2007-6750
  Apache バージョン 1.x 系及び 2.x 系に含まれている DoS の脆弱性．この脆弱性を悪用した攻撃のツールとして，Slowloris がある [20]．

攻撃端末と，被害端末の環境を表 4 に示す．

表 4　攻撃端末及び被害端末の環境

	OS 名	ソフトウェアのバージョン
攻撃端末の環境	Ubuntu 16.04	-
被害端末の環境	CentOS 6.7	Bash 4.1.2 Apache 2.2.15

4.2 Web サーバに対する攻撃体験演習

本演習は，4.1 節で示した 3 つの脆弱性を悪用した攻撃を，ツールを用いて受講者が体験する演習である．

あらかじめ，提案システム内の攻撃端末には，攻撃用のツールが準備されているので，受講者は攻撃端末上でツールを実行するだけで，Web サーバを停止させる攻撃の体験が可能である．

これにより，Web アプリケーションにおける，ミドルウエアや OS への攻撃の体験演習が可能となる．特に，Web アプリケーションにおいては，アプリケーションそのものへの脆弱性診断が多いが，それ以外に，ミドルウエアや OS への脅威があることを体験的に知ることができる．

5. 提案システムの運用管理

5.1 C/R の複製

C/R は 1 セットで 2 人が同時に演習を行うことを想定した環境なので，複数の受講者が同時に演習を行う場合，演習前に，C/R を複製する必要がある．

複製は，C/R が動作しているクラウド上で，図 10 でのサイバーレンジ管理用インスタンスから，クラウド事業者が提供するクラウド基盤に複数の命令を送信することで行う．C/R を複製する際は，C/R を構成している仮想マシンが使用している仮想ディスクの状態の他に，仮想マシンのプライベート IP アドレスや F/W の設定を含むネットワークの設定等が引き継がれるので，複数の受講者は，同一の環境で演習をそれぞれ行うことができる．

C/R の複製時には，複製元とは別のグローバル IP アドレスを新たに取得し，その IP アドレスをサイバーレンジ接続用 PC に割り当てることで，受講者はそれぞれ別の C/R で演習ができるようになっている．

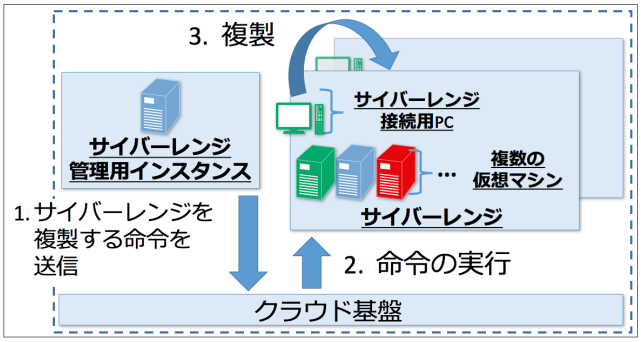

図 10　C/R の複製の概要図

5.2 管理者インターフェースについて

学習支援システムには管理者用のインタフェースが用意されているので，コース枠の作成，コース毎のコンテンツの作成，及び，問題の作成ができる．提案システムでは，独自の確認テストのため一部，Moodle を改変している．

また，管理者は，このインタフェースから受講者の進捗や確認テストの点数を確認することができる（図 11）．

6. 運用実績・評価

6.1 運用実績

2018 年 5 月までの約 3 年で，約 300 名の受講者が演習を行った．最大で 8 セットの C/R（合計 104 台の仮想マシン）を同時に稼働させて演習を行ってきたが，大きなトラブルはなかった．

6.2 提案システムの稼働時間及び複製にかかる時間の評価

C/R の複製に必要な時間を複数回測定し，評価を行っ

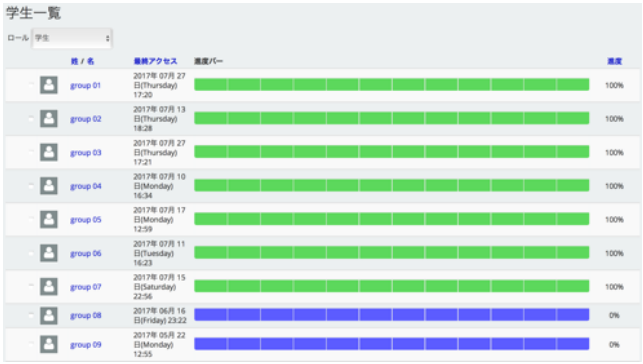

図 11　管理者用インターフェース

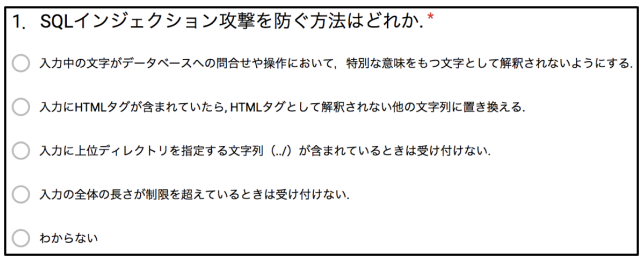

図 12　理解度テストの問題例

た．測定は，図 10 に示した C/R の複製をするためのスクリプト（以後，複製スクリプトと呼ぶ）を用意し，それを実行することで行った．

複製スクリプトを実行し始めてから，複製が終了したことを示す応答がクラウド基盤から返されるまでの時間を計 100 回測定し，その平均値を計算した．計算の結果，複製にかかる時間の平均は，752 秒となった．これは実運用上問題のない結果と言える．

6.3　提案システムでの演習の学習効果の評価

提案システムでの演習を受講した者約 300 名のうち，大学生 33 名，社会人 18 名，中学生及び高校生 29 名を対象に，演習内容の理解度を測るテストや，アンケートを行い，提案システムの学習効果を評価した．評価の結果を表 5 に示す．

6.3.1　大学生を対象とした理解度テストを用いた評価

提案システムの学習効果について，情報処理技術者試験等の公的試験 [21] を参考に作成した問題を使用して理解度テストを行い，提案システムの学習効果の評価を試みた．

明治大学理工学部に在籍する学部 3 年生及び 4 年生 33 名に提案システムでの演習を受けてもらい，理解度テストを演習前後で行った．出題数は 10 問であり，1 問 1 点で採点をした．理解度テストは，標的型攻撃編および SQL インジェクション編に関連した内容となっており，多肢選択法で行った．理解度テストの問題例を図 12 に示す．

理解度テストを実施した結果，演習実施前の 33 名の理解度テストの平均点は 3.94 点であったのに対し，演習実施後の平均点は 6.27 点（+2.33 点）となった．これにより，学習効果があったことが確認できたと言える．

6.3.2　社会人を対象とした理解度テストを用いた評価

提案システムを用いた演習を社会人 18 名を対象に行った．18 名のうち，8 名は 10 点満点の理解度テストを実施し，10 名は 7 点満点とした理解度テストを実施し，提案システムの学習効果の評価を試みた．

その結果，10 点満点の理解度テストを受けた 8 名の，演習実施前の平均点は 8.36 点であり，演習実施後の平均点は 9.50 点（+1.14 点）であった．同様に，7 点満点の理解度テストを受けた 10 名の，演習実施前の平均点は 4.30 点であり，演習実施後の平均点は 4.80（+0.50 点）であった．

18 名のうち 5 名は，理解度テストの点数が演習実施前の点数と比較して，演習実施後の点数が若干下がっていた．これは，被験者が理解度テストの問題を理解せずに選択した結果，試験結果に揺れが生じたためであると推察される．

10 点満点の理解度テストを受けた 8 名は，セキュリティに携わる仕事をしている方々であり，演習実施前時点である程度のセキュリティに関する知識を有していたと考えられる．そのため，演習実施前の理解度テストの平均点が比較的高く，演習後の平均点が大きく増加しなかったと考えられる．

6.3.3　中高生を対象としたアンケートを用いた評価

提案システムでの演習の一部である，標的型攻撃体験演習（図 7 参照）のみを切り出した演習を中高生 29 名に受けてもらい，標的型攻撃の体験演習の評価を試みた．この演習が，標的型攻撃に対する受講者の理解度の向上に貢献しているかどうかを，アンケートを用いて評価した．

演習の前後で以下の A，B に示す質問に 1 から 10 の整数で回答してもらった．なお，回答が 1 の場合は”全くできない”，10 の場合は”できる”を示している．つまり，数値が大きいほど，標的型攻撃に対する理解度が高いということになる．

（A）　標的型攻撃はどのように感染するのか等の「仕組み」を，他の人に説明できますか．

（B）　標的型攻撃を受けるとどのような「被害」に遭うのかを，他の人に説明できますか．

評価の結果，演習実施前の問 A の平均点は 1.65 点であり，演習実施後の平均点は 6.43 点であった．同様に，演習実施前の問 B の平均点は 2.14 点であり，演習実施後の平均点は 7.17 点であった．このことから，受講者の標的型攻撃に対する理解度が，演習を通して向上したことが示された．

6.3.4　研究倫理について

提案システムを用いた演習の一部では，サイバー攻撃の方法を学ぶ．その知識を悪用すると，他者への被害を招き犯罪行為となる可能性がある．よって，受講者，特に学生に対しては，演習の最初に，知識を悪用しないように注意

表 5　学習効果の評価結果

実施形態	受講者	回答者数	評価		平均点	
			手法	問題数/問題の種類	演習前	演習後
大学実習	大学生	33 名	理解度テスト	10 問	3.94 点/10 問中	6.27 点/10 問中
社会人向け	社会人	8 名		10 問	8.36 点/10 問中	9.50 点/10 問中
セミナー		10 名		7 問	4.30 点/7 問中	4.80 点/7 問中
中高生向け	中高生	29 名	アンケート	問 A	1.65 点/10 点中	6.43 点/10 点中
セミナー				問 B	2.14 点/10 点中	7.17 点/10 点中

喚起をした．また，中高生の演習の際には，若年層のサイバー犯罪についてのディスカッションを行い，同世代のサイバー犯罪の動機等についてを議論した．

提案システムの評価のため，受講者からアンケートや成績を集積した．これらの情報には個人を特定する情報はないが，その情報は最適だと思われる方法で管理し，管理データについてもセキュリティ対策を施している．

今後も引き続き，演習前の，悪用についての注意喚起の徹底と，個人情報を含む情報管理の徹底を行うこととする．

7. まとめ

本論文では，初学者を対象とした体験型サイバーセキュリティ学習システムを提案し，その評価を示した．

提案システムの狙いとしては以下の通りであり，これらを達成できたと言える．

- 初学者向けの体験型のサイバーセキュリティ演習を提供すること
- 演習を実施する際のインストラクターの負担を下げること
- インストラクターが不在でも自習が可能であること
- 時間や場所の制約を受けずにシステムの利用が可能であること
- 受講者の数が増えても対応可能であること

提案システムにおいて，1 セットの C/R を複製するのに必要な時間は平均 752 秒であり，実運用上問題がないことが示せた．また，約 3 年の運用で，システム上の大きなトラブルは発生しなかった．

演習による学習効果を評価した結果，大学生を対象とした理解度テストの平均点が 2.33 点向上するなどし，特に，初学者に対して，提案システムの学習効果が確認できたと言える．

謝辞

本研究の一部は，レンジフォース株式会社の支援により実施している．

横山雅展氏には，研究及び論文作成上で支援をいただいた．記して感謝する．

参考文献

[1] 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
[2] 実践的サイバー防御演習「CYDER」，https://cyder.nict.go.jp/
[3] 「金融業界横断的なサイバーセキュリティ演習（Delta Wall ）」について，http://www.fsa.go.jp/news/29/sonota/20171020/20171020-1.html
[4] 八代 哲，高橋 和司，渡辺 亮平，角田 裕太，田邉 一寿，横山 雅展，齋藤 祐太，齋藤 孝道，”体験型サイバーセキュリティ学習支援システムの提案と構築”，コンピュータセキュリティシンポジウム 2017,2017.
[5] SQL インジェクション対策について，https://www.ipa.go.jp/files/000024396.pdf
[6] 標的型攻撃/新しいタイプの攻撃の実態と対策，https://www.ipa.go.jp/files/000024542.pdf
[7] 平成 28 年中におけるサイバー空間をめぐる脅威の情勢等について，https://www.npa.go.jp/publications/statistics/cybersecurity/data/H28cyber_jousei.pdf
[8] 情報セキュリティ 10 大脅威 2017，https://www.ipa.go.jp/files/000058504.pdf
[9] 2016 年度情報セキュリティの脅威に対する意識調査，https://www.ipa.go.jp/files/000056568.pdf
[10] 安全なウェブサイトの作り方改訂第 7 版，https://www.ipa.go.jp/files/000017316.pdf
[11] JPCERT コーディネーションセンター，https://www.jpcert.or.jp/ir/
[12] コンピュータセキュリティインシデント対応ガイド，https://www.ipa.go.jp/files/000025341.pdf
[13] 情報セキュリティの現状と動向について-サイバー演習の実施要領と演習事例-，https://ssl.bsk-z.or.jp/kakusyu/pdf/27-1jyouhousekyurithityousakennkyuu.pdf
[14] Moodle，https://moodle.org/
[15] metasploit，https://www.metasploit.com/
[16] Adobe Flash Player の脆弱性対策について（APSB15-03）（CVE-2015-0311 等），https://www.ipa.go.jp/security/ciadr/vul/20150128-adobeflashplayer.html
[17] Internet Explorer の脆弱性の修正について（MS11-003），https://www.ipa.go.jp/security/ciadr/vul/20110209-ms11-003.html
[18] CVE-2011-3192，http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192/
[19] CVE-2014-6271，http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271/
[20] CVE-2007-6750，http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750/
[21] 情報処理技術者試験・情報処理安全確保支援士試験，https://www.jitec.ipa.go.jp/