

オンライン公開講座としての サイバーセキュリティ堅牢化演習の運営

丸山 一貴^{1,a)} 佐々木 伸彦² 高谷 宏幸^{3,4} 末田 欣子¹

受付日 2021年11月16日, 再受付日 2022年3月3日,

採録日 2022年4月22日

概要: サイバーセキュリティに興味を持っているものの、具体的な学びの入口が分からないと考える高校生・大学生を主な対象として、実践的な演習を伴う無償の公開講座を年に1回開催してきた。2020年度は、ITサービスを運営しながら脆弱な状態を解消していく堅牢化を題材として取り上げることが計画していた。従来は演習環境を整えたノートPCを本学で用意して参加者に提供していたが、新型コロナウイルス感染症の拡大により対面型の講座を開催できなかったため、すべての活動をオンラインで実施することに決定した。演習環境は仮想環境上に構築して、そのデスクトップにはWebブラウザでアクセスし、資料の提供には本学の学習管理システムを、公開講座運営にはZoomを、参加者のチーム内コミュニケーションにはSlackを活用した。本稿では、演習を伴うオンライン公開講座の要件を整理し、オンラインツールを組み合わせた実装と運用の経験や課題を述べ、知見を共有することを目的とする。

キーワード: サイバーセキュリティ教育, オンライン演習環境, 仮想マシン, Zoom, Slack

Virtual Public Lecture Operation of Cyber Security Hardening Practice

KAZUTAKA MARUYAMA^{1,a)} NOBUHIKO SASAKI² HIROYUKI TAKATANI^{3,4} YOSHIKO SUEDA¹

Received: November 16, 2021, Revised: March 3, 2022,

Accepted: April 22, 2022

Abstract: We held the annual free public lecture on cyber security practice for high school and undergraduate students, who are interested in, but not introduced to cyber security. In 2020, the theme of the lecture was *hardening*, fixing some vulnerabilities on a target system to keep it running. Until 2019, we provided laptop PCs with a vulnerable system to each attendee. Since COVID-19 prevents us from holding a usual on-site event in 2020, we decided to hold it as a fully virtual one. The target system of hardening was deployed as a virtual machine. The attendees accessed the desktop of the system with their web browser, and the reference materials through our learning management system. The lecture was provided on Zoom and the attendees also used Slack for communicating with each other. In this paper, we describe the requirements of such virtual event, the implementation with some online tools, our experiences in operating the event, and the remaining problems to share our knowledge.

Keywords: cyber security education, online cyber range, virtual machine, Zoom, Slack

1. はじめに

サイバーセキュリティの重要性は、テレワークの定着や教育におけるICT活用の拡大といった情勢の変化に応じて一層増大しており [1]、関連する話題がマスメディア等で広く報道されることも多い。一方で、一般の人にとっては高度に複雑で難しいものと思われがちであり、また、報道される際には事件性の部分に重きが置かれることも多

¹ 明星大学

Meisei University, Hino, Tokyo 191-8506, Japan

² ストーンビートセキュリティ株式会社

Stonebeat Security, Inc., Chiyoda, Tokyo 102-0083, Japan

³ McAfee Enterprise, Shibuya, Tokyo 150-0043, Japan

McAfee Enterprise, Shibuya, Tokyo 150-0043, Japan

⁴ 現在, Trellix

Presently with Trellix

^{a)} kazutaka@acm.org

く、サイバーセキュリティへの理解を深めたり、学びの入口を示したりすることにはつながっていない。サイバーセキュリティの教育については、企業では社内教育の一環として演習付きの研修を行うか、外部に委託して実施している。大学生等にとっては専門的なカリキュラムを持つ学科で学んだり、CTF (Capture The Flag) のような競技大会を目指してトレーニングを行ったりすることが多いが [2], [3], 興味を持ち始めた入門者が入口とするにはいずれも気軽に参加することが難しいと言える。サイバーセキュリティに関わるためにはプログラムや OS, ネットワークといった幅広い分野の理解が必要なことから、学生が自身の専門分野を活かしたり、その他の分野に興味を持つことの必要性を感じることも重要であると考えている。そこで、我々は 2015 年度から 10 代の生徒・学生を主な対象として、実践的なサイバーセキュリティ演習を無償の公開講座として実施してきた [4]。

2019 年度までは明星大学の教室を使用して対面型で行ってきたが、2020 年度は新型コロナウイルス感染症の拡大によって対面型での実施が困難になったため、公開講座の説明や演習環境の提供、参加者のサポートを全てオンラインに移行して実施することとなった。具体的には、仮想環境上に構築した演習環境と本学の学習管理システム (以下、LMS という)、Zoom, Slack を組み合わせることで実現した。本稿では、演習を伴うオンライン公開講座の要件を整理し、オンラインツールを組み合わせた実装と運用の経験や課題を述べ、知見を共有することを目的とする。

2. 公開講座の要件と解決策

本章では、我々が運営してきた公開講座における演習の概要と要件について述べるとともに、対面型とオンライン型それぞれにおける解決策を説明する。

2.1 演習の概要と要件

公開講座の参加者には、実機を用いた演習を伴う演習参加者と、講演を聴いて演習を観覧する聴講参加者の 2 種類がある。演習参加者は 3 名 1 組でチームを構成し、チームメンバーが協力して課題に取り組む形式を取る。聴講参加者は、演習参加者が課題に取り組む様子を見ながら、進行役を務める講師の補足説明を聞く形式である。公開講座全体は講演と演習に分かれており [4], 演習で実際に手を動かすことには興味や自信がない参加者や、講演を聴くことが主たる目的の参加者向けに、聴講参加者のカテゴリーを設けて区別している。

演習は大きく前半と後半に分かれた構成としており、前半は前提知識やツール類の紹介をハンズオン形式で行い、後半はその経験を利用して課題に取り組んでチームごとの成果を競う。演習の題材は毎年異なるが、サイバー攻撃や

デジタルフォレンジックスに関するものを選定し、実際のツール使用やログの調査を伴う内容としている。たとえばサイバー攻撃を題材とする場合、1 つの課題をクリアすると次の課題に取り組めるよう、連続する小規模な課題の集まりとして構成している。課題の設定にあたっては、入門者向けという観点と、単なる作業だけで終わらずサイバーセキュリティの対策に活かすという観点から、以下の 2 点に留意している。

- シェル等のコマンド操作を体験したことがない演習参加者もいることから、多くのコマンドを実行する課題はなるべく避ける。課題で必要となるコマンドの使用法は演習前半のハンズオンで取り扱い、その資料がヒントになるよう構成する。
- 演習の時間の終わりに、題材として取り扱ったインシデントの原因や、そう判断した根拠、再発させないための対策を簡単な報告書としてまとめてもらう。

演習の終了後は内容の講評と全体の総括を行う。その際、チームごとの課題の到達度と、作成した報告書の内容を考慮して、優秀な成果を上げたチームを表彰することとしている。

入門者向けと位置づけた公開講座の実施にあたっては、参加者にサイバーセキュリティ分野の前提知識を要求しないこと、チームメンバーがいない個人であっても申し込めることに配慮する必要があると考えた。これらを踏まえ、以下の要件を設定した。以降の節で、それぞれの解決策を述べる。

- (1) 主催者が、演習参加者の前提知識・技術レベルの差異を吸収する機会を提供すること。
- (2) 主催者が、演習参加者にチームビルディングの機会を提供し、課題に取り組みやすくすること。
- (3) 演習参加者が、チームで手分けしながら演習に取り組めること。
- (4) 演習参加者が、課題への取り組みで行き詰まった場合にアドバイスを求められること。
- (5) 聴講参加者が、演習参加者の課題への取り組み状況を把握できること。

2.2 対面型での解決策

図 1 は、本学の 1 教室に集まって対面型の公開講座を実施している様子である。教壇には演習を進行する講師役が登壇し、教室内の音響設備と授業用の教材提示装置を使用して説明を行う。机は島形に配置し、演習参加者の 1 チーム 3 名が 1 つの島を占有して利用できる。島にはノート PC を 3 台設置し、それぞれに演習環境を構築している。聴講参加者の座席は教室の壁沿いに設けているが、課題に取り組む演習の後半では教室を自由に移動することが可能で、講師の説明を聞きながら各チームの様子を見比べることができる。



図1 2019年度の公開講座の様子
Fig. 1 Public lecture in 2019.

2.1節で述べた要件(1)については、その年の課題の内容に合わせた予習用の教材を開催日より前に提供し、知識不足を各自に補ってもらったこととした。資料は明星大学が運営するLMSに掲載し、演習参加者にゲストIDを発行することでアクセスできるようにした。また、教材の内容に関する簡単なドリル問題を設定して、参加者が理解度を確認できるようにした。

要件(2)については、演習参加の申し込み方法に関係している。演習参加の申し込みは1名や2名で行われることもあり、我々、運営側が所属や学年等を考慮したうえで、3名1組となるように組み合わせている。従って、公開講座当日に初めて出会った3名でも課題に取り組みやすくなるよう、公開講座の進行が演習後半に達するまでに自己紹介の時間を設けるなど、アイスブレイクの機会が持てるよう配慮した。

要件(3)については、1人1台の演習環境を用意することで解決した。1人1台の操作端末から同一の演習環境を共有するという選択肢もあるが、同じ設定ファイルに対して他のメンバーとは異なる変更を試みる場合も考えられることから、メンバーごとに独立した演習環境とした。前述のとおりチーム単位の島となっていることから、他のチームメンバーに自分の画面を見せることで、スムーズに情報共有を行うことができる。

要件(4)については、演習参加者の質問に対応するためのスタッフを数名、教室内に配置して巡回した。公開講座の教材や演習環境の準備は、公開講座を後援するストーンビートセキュリティ(株)の協力を受けており、対面型の公開講座では運営補助のスタッフとして現地でも協力を受けていた(以下では、筆者らと後援企業の運営補助者を合わせて運営スタッフという)。演習参加者は最大10チーム・30名であり、手を挙げてサポートを求めることができる。プログラミング等の演習型授業における、TAのような位置づけである。

要件(5)については、講師によりチームごとの状況を随時説明したり、Facebook CTF^{*1}を利用した可視化を試みたりしてきたが、演習参加者向けの進行の説明も並行して行う必要があり、適切な解決には至っていなかった。

2.3 オンライン型での解決策

2020年度の公開講座をオンライン型で実施するにあたり、2.1節の各要件に加えて、以下の要件を考慮する必要があった。

- (6) 教室内の音響設備と教材提示装置による説明・進行を代替する仕組みがあること。
- (7) 演習参加者が、オンライン型で使用する演習環境やコミュニケーションツールの利用方法を事前に習得できること。

オンライン型におけるこれら各要件の解決方針について述べる。要件(1)については、対面型と同様に予習用教材をLMS上に掲載することで解決した。オンライン型ではこれを事前課題と位置づけ、公開講座の約2週間前に提供を開始した。事前課題の内容は、公開講座当日の演習で取り組む課題の一部に関連した内容とし、対象となる脆弱性に関する基礎知識の習得や、使用するコマンド、修正する設定ファイルに触れるものとなっていた。演習参加者が実際にコマンド操作等を行えるようにするため、公開講座当日の演習で使用する環境に近い状態のオンライン演習環境を作成し、事前課題の内容に合わせてセットアップした状態で演習参加者に提供した。演習参加者は事前課題に取り組み、LMS上に設定した小テストに解答する形でアウトプットを行うこととした。小テストへの解答内容は後述する学生スタッフ(要件(4)で述べる)が確認し、誤りがあればヒントを提示して正解に導くようにすることで、公開講座当日にどこから手を付けていいかわからないという状況を避けることを目指した。

要件(2)については、前述の事前課題を演習参加者のチームメンバー同士が相談しながら取り組めるよう、後述するコミュニケーションツール(要件(6)で述べる)を提供した。また、後述する学生スタッフが声かけを実施したり、提出された小テストの内容をチェックして、評価をフィードバックすることでチーム内のコミュニケーションが発生するよう誘導した。

要件(3)については、対面型でのノートPC上に構築した演習環境の代替として、オンライン演習環境を仮想環境上に構築し、1人が1台のOSインスタンスを占有できる状態にした。事前課題の期間に画面の内容をチーム内で共有するには、コミュニケーションツールを使用するか、演習環境のデスクトップのアクセス権を共有することで解決した。後者の詳細は4章で述べる。公開講座当日はこれ

*1 <https://github.com/facebookarchive/fbctf>

らに加え、各チームごとに独立した Zoom のブレイクアウトルームを作成し、Zoom での音声や画面共有による連携も併用可能な状態とした。

要件 (4) については、サイバーセキュリティに興味のある明星大学情報学部生が授業の一環として質問対応スタッフ（以下、学生スタッフという）の役割を果たした。学生スタッフは 3 名 1 組に構成し、各組が演習参加者の複数のチームを担当するよう割り当て、事前課題から公開講座当日まで、一貫して対応した。学生スタッフが解決できない質問は、運営スタッフにエスカレーションして指示を仰ぎ、その内容を演習参加者に回答する運用とした。

要件 (5) については、講師による聴講参加者専用の解説と、状況を把握するダッシュボードの表示を活用した。対面型では教室内の音響設備を (a) 聴講参加者向けの解説と、(b) 演習参加者向けの進行のアナウンスとの両方に使用しており、講師 1 名がその両方を担わざるを得なかった。オンライン型では (a) に Zoom のメインルームを使用し、説明担当の講師は聴講者向けの説明に専念した。(b) は後述するコミュニケーションツールで代用し、アナウンスは学生スタッフ等、説明担当の講師以外が行った。聴講参加者向けの説明では、演習参加者の各チームが課題をどの程度クリアしているかを把握しやすくするため、図 2 のようなダッシュボードを用意して Zoom のメインルームで画面共有し、聴講参加者に示した。ダッシュボードはマトリクス状になっており、1 行が演習参加者 1 名に、1 列が堅牢化して防御すべき脆弱性の課題に対応している。緑のセルが解消した脆弱性を、赤のセルが未対応の脆弱性を示している。ダッシュボードの実装については第 4 章で述べる。

要件 (6) については、ビデオ会議システム Zoom とコミュニケーションツール Slack を併用した。Zoom は公開講座当日のみに使用し、演習前半までの運営はメインルームで、演習後半はブレイクアウトルームを作成して演習参加者のチームごとに割り当てた。メインルームには運営スタッフと聴講参加者が、ブレイクアウトルームには演習参加者がチームごとに参加した状態となる。演習終了後の講



図 2 ダッシュボードの表示例

Fig. 2 Example of the dashboard.

評等は、ブレイクアウトを終了して全員がメインルームに戻った状態で行った。Slack は、事前課題の取り組みで演習参加者のチームメンバー同士が交流するとともに、学生スタッフとのやり取りで利用した。事前課題ではチームごとに公開チャンネルを作成し、事前課題を提出したら学生スタッフにメンションして知らせ、チェックを受ける手続きにした^{*2}。公開講座当日はチームごとに非公開チャンネルを作成し、チームメンバーと運営スタッフ、学生スタッフをメンバー登録した。演習参加者は Zoom のブレイクアウトルームを使用した音声でのやり取りに加え、この非公開チャンネル内でスクリーンショットやコマンド列を共有することができる。課題に行き詰まった際は、学生スタッフへメンションして問い合わせを行い、アドバイスを求める。運営スタッフは、学生スタッフからエスカレーションがあった場合に非公開チャンネル内の書き込みを確認するとともに、余裕のある時間帯はチームメンバー同士のやり取りを見て、ダッシュボードに現れない進行状況を確認した。

要件 (7) については、特にオンライン演習環境へのアクセス方法と、Slack の利用方法について、事前の習得が必要であると考えた。LMS は一般的な Web システムであること、Zoom はオンライン授業等を通じて演習参加者も利用経験があると考えられることから、特に対策を行わなかった。一方で、オンライン演習環境は Web ブラウザを通じて仮想マシンのデスクトップにアクセスする方式である（詳細は 4 章で述べる）。公開講座当日の時間を節約するため、オンライン演習環境への具体的なアクセスとログインの方法は、演習参加者に事前に習得してもらう必要がある。また、演習参加者が使用する Web ブラウザやキーボード配列との組み合わせによっては操作に支障が発生する可能性があるため、その確認とフォローアップも事前に行う必要があった。Slack は公開講座当日に学生スタッフへアドバイスを求める際に使用するの、一般的なスレッドや通知の説明に加えて、特にメンションの使い方を習得してもらうことに留意した。事前課題の提出時に学生スタッフへメンションする手続きにしたのは、このためである。オンライン演習環境については運営スタッフが、Slack については学生スタッフが、それぞれ利用方法の簡易な資料を用意し、事前課題の開始に合わせて LMS で演習参加者に提供した。

3. オンライン公開講座の運営

本章では、2.3 節で述べた解決策を実装したオンライン公開講座の、当日の運営について述べる。

^{*2} Slack は、ユーザーグループ機能を利用するため、月額の有償プランを使用した。たとえば、チーム A のサポートを担当する学生スタッフを 1 つのユーザーグループにまとめ、チーム A の演習参加者はそのグループ宛にメンションを行う。

3.1 公開講座のシステム構成

図3に、公開講座当日に演習後半を運営している際のシステム構成を示す。2.3節で述べたとおり、演習参加者は自身のチームに割り当てられたZoomのブレイクアウトルームと、Slackの非公開チャンネルに参加している。LMSを通じて、事前課題の資料にもアクセス可能である。また、図中にアナウンス用と示したSlackチャンネルは、演習参加者、聴講参加者、運営スタッフのすべてが参加しているが、参加を意味する配線は記載を省略した。

彼らを支援する学生スタッフは、Slackの各チーム専用チャンネルを通じて問い合わせを受ける。Zoomでは学生スタッフ専用のブレイクアウトルームを作成し、学生スタッフ同士が音声で情報共有できる状態にした。運営スタッフのうち筆者ら講師と、聴講参加者はZoomメインルームに参加して、聴講参加者向けに課題の内容や各チームの進捗状況等を共有した。講師以外の運営スタッフはSlackの各チーム専用チャンネルに参加してはいるが、演習参加者と直接のやり取りはほとんど行わないため、図中では記載を省略している。

運営スタッフ同士は、任意のタイミングで講座運営に関する情報共有が必要になるため、ZoomやSlackに依存せず、明星大学情報学部の会議室に集合し、運營業務に従事した(図4)。4章で述べるオンライン演習環境が動作する機材はストーンビートセキュリティ(株)が管理する区域に設置したため、運営スタッフの一部はこの会議室ではなく当該設置箇所で運營業務に従事した。学生スタッフは各自の自宅からオンラインで参加し、演習参加者から受けた質問を運営スタッフにエスカーションする際は、図3

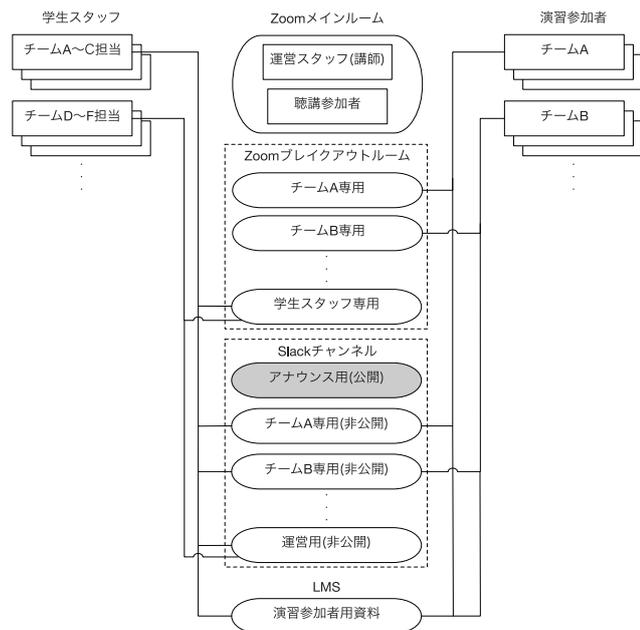


図3 オンライン公開講座の演習運営時のシステム構成

Fig. 3 System architecture in the practice of the virtual public lecture.

の運営用チャンネルを通じて連絡を取り合った。なお、図中で運営スタッフと運営用チャンネルの配線は記載を省略している。

3.2 堅牢化演習の概要

題材として設定した堅牢化演習では、複数の脆弱性を有する架空のeコマースサイトを対象として、外部からそれら脆弱性への攻撃が継続的に実施されている状況を設定した。

各チームの到達度を定量的に比較するため、サイトが正常に稼働している場合は売り上げが伸び、脆弱性への攻撃が成功すると販売が阻害され損失が出るとみなして、売り上げから損失を引くことでスコアを算出することとした。これにより、より早く、より多くの脆弱性を対処できたほうが、多くの売り上げと少ない損失によってスコアが高くなる。脆弱性の中には、正しい対策を取らないと繰り返し発現するものが用意してあるため、一時的に解決するだけの誤った対策を行うと損失が継続するようになっている。

演習参加者の脆弱性への対応状況を時間軸に基づいて確認できるよう、チャート形式の表示も準備した(図5)。



図4 オンライン公開講座の運営時の会議室

Fig. 4 Meeting room as an operation center of the virtual public lecture.



図5 チャートの表示例

Fig. 5 Example of the chart.

表 1 チームの編成状況

Table 1 Details of the teams.

チーム	生徒・学生 (名)	社会人 (名)	知人同士の数 (名)
A	3	0	2
B	2	1	3
C	3	0	3
D	3	0	3
E	3	0	2
F	3	0	3
G	2	1	1
H	3	0	3
I	0	3	3
J	0	3	1

左上の折れ線グラフは横軸が時間、縦軸がスコアを表しており、演習参加者が適切な対策を取ったタイミングが把握しやすくなっている。

3.3 演習参加者の概要

演習参加者の申し込み枠は 30 名であり、生徒・学生 22 名、社会人 8 名の事前申し込みがあった。2.2 節のとおり、3 名未満で申し込みがあった場合は所属や学年等を考慮して組み合わせ、A から J の 10 チームに編成した。申し込みにあたって収集する個人情報には年齢や事前知識の有無を含まないため、生徒・学生の場合は所属が高校か大学か、同じ学校か否かを、社会人はなるべく社会人同士となることを基準とした。編成後の各チームの内訳を表 1 に示す。表中の知人同士の数は、3 名で申し込んだ場合は 3、2 名と 1 名の申し込みだった場合は 2、1 名ずつの申し込みだった場合は 1 と記載した。

4. オンライン演習環境の構成

本章では、2.3 節で述べたオンライン演習環境の実現方式について述べる。

図 6 にオンライン演習環境の構成図を示す。演習参加者が使用する演習環境は VMware ESXi 上の仮想マシンとして構成した。仮に一部の仮想マシンが高負荷になってもその影響を限定的にすることと、可用性を確保することを目的として、仮想マシンを動作させるサーバは 2 台に分散させることとした。演習環境用サーバの構成は表 2 のとおりであり、表 3 のように各サーバ上に仮想マシンを配置した。バックアップ用 VM の仮想ディスクは、本来であれば仮想マシンのライブマイグレーションが可能のようにサーバ間で共有すべきであるが、今回は簡略化のため演習開始時点のものをコピーして静的に保持した。

演習参加者から各サーバへのネットワークもサーバごとに分割し、ダウンリンク最大 2 Gbps、アップリンク最大 1 Gbps の回線をそれぞれに用意した。なお、試験的に負荷をかけて計測した際の実測値は、いずれもダウンリンク

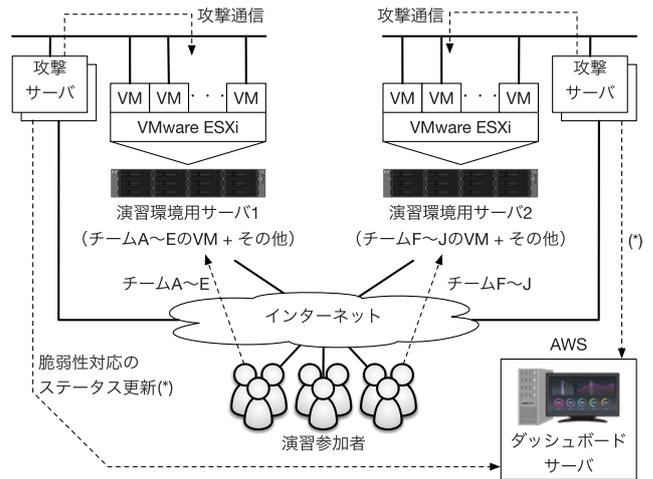


図 6 オンライン演習環境の構成

Fig. 6 System architecture of the practice environment.

表 2 演習環境用サーバの構成

Table 2 Configuration of the servers for the practice environment.

ハードウェア	下記仕様のサーバ 2 台で構成
CPU	Intel Core i7 10700K 3.80GHz (8 コア)
Memory	64GB (DDR4-3200MHz)
SSD	2TB
ハイパーバイザ	VMware ESXi Server 6.7
仮想マシン	下記仕様の仮想マシンを合計 36 台で構成
CPU	1 コア
Memory	2GB
ゲスト OS	CentOS 7

表 3 仮想マシンの割り当て

Table 3 Assignment of the virtual machines for each team.

サーバ 1	チーム A~E 用 VM 15 台 学生スタッフ用 VM 3 台 サーバ 2 のバックアップ用 VM 21 台
サーバ 2	チーム F~J 用 VM 15 台 学生スタッフ用 VM 3 台 運営スタッフ用 VM 3 台 サーバ 1 のバックアップ用 VM 18 台

900 Mbps, アップリンク 700 Mbps 程度であった。各サーバのバックエンド側には、演習参加者の各 VM に対してサイバー攻撃を実施する攻撃サーバを二重化してそれぞれに配置し、低速安価な別のアクセス回線を通じてインターネットに接続した。

攻撃サーバ上に、攻撃を試行する Python スクリプト (平均して 40 行程度) を各脆弱性ごとに作成して、一定間隔で自動的に実行させた。応答の内容やタイムアウトといった実行結果から、攻撃の成否、すなわち脆弱性の修正状況を自動的に判定することができる。攻撃の成否は、対象の演習環境を使用するユーザ ID と、脆弱性を区別する

ID と合わせて、攻撃サーバから AWS 上に構築したダッシュボードサーバへ HTTPS の GET メソッドを使用して送信される。ダッシュボードサーバでは Apache および MariaDB を動作させるとともに、攻撃サーバから受信したデータを集計して図 2 や図 5 のように表示するプログラムを、Web アプリケーションフレームワークである Django を利用して実装した。主要な機能で 1000 行程度のコード量である。

演習参加者は自分のチームに割り当てられた VM のデスクトップに、VMware ESXi の Web インタフェースを通してアクセスする。各チームに発行された ID は、割り当てられた VM の起動・停止等に限定された権限が設定されている。対面型では、ノート PC の画面をのぞき込むことで画面内の情報を共有していたが、オンライン型ではこの Web インタフェースで他のメンバーが使用する VM のデスクトップにアクセスすることができる。しかし、この方法では VM へのキー入力等を共有する形になり、後から接続した（デスクトップをのぞき込んだ）ユーザの偶発的なキー入力、先に接続していた（当該デスクトップで作業中の）ユーザの操作を邪魔してしまう可能性がある。このため、Zoom により音声で状況を共有しながら、デスクトップをみられる側が主体的に Zoom で画面共有したり、Slack にスクリーンショットを書き込んだりするほうが、短時間で実施する演習ではトラブルが少なく現実的であると考えている。

演習環境は 1 人 1 台としたことで、3 名 1 組のチームに同一の演習環境が 3 台あり、同じ脆弱性がそれぞれの演習環境に準備されている。ダッシュボードサーバではこれらと同じ脆弱性を別々に集計する仕様としたため、チームの誰かがある脆弱性の修正方法を発見すると、Zoom による音声か Slack への書き込みによりその情報を共有し、他のメンバーも各自の演習環境でその脆弱性を修正する、という進め方を今回は採用した。

5. 評価と考察

本章では、オンライン型での公開講座運営について、2.3 節で設定した解決策の有効性や、実際の運営を通じて得られた知見について述べる。

5.1 オンライン型の要件に対する解決状況

2.3 節で述べた 7 つの要件をどの程度解決できたかについて、事前課題の期間、公開講座当日の演習前半、演習後半という 3 つのタイミングに整理して述べる。

事前課題の期間は、公開講座当日である 2020 年 12 月 20 (日) から約 2 週間前の、12 月 5 日 (土) から開始した。LMS へのアクセス方法をメールで通知し、掲載した資料を読んで Slack に登録後、事前課題に取り組むという流れである。演習参加者のうちキャンセルなく公開講座当

日に参加したのは 22 名、うち 13 名が翌 6 日には Slack への登録を完了した。事前課題への着手時期は各参加者の事情により様々であったが、オンライン演習環境へのアクセス方法や Slack の利用で特に問題は発生しなかった。一部の参加者は、Slack の #random チャンネルでチームを超えて自己紹介や雑談をするなどの交流がみられたこと、セキュリティの題材に馴染みのある参加者や社会人の参加者がリーダーシップを取ってくれる事例がみられたことは前向きな評価と言える。一方で、知人同士で申し込んだ場合は Slack 上の交流が不要であり、また初対面同士では簡単な挨拶程度のやり取りであったことから、短期間で初対面の参加者同士を盛り上げるファシリテーターの役割が不足していたと言える。ファシリテーターのスキルを持つ運営スタッフもしくは学生スタッフを配置し、初対面の参加者同士のチームビルディングを支援することが必要である。なお、優秀な成果を上げて表彰対象となったチームは E, H, I の各チームであり、いずれも当日に全員が参加し、メンバーに知人が含まれていたチームである。事前課題の内容と分量・提供期間についてのアンケート結果を表 4 に示す。分量と期間は適切であったが内容については評価が分かれており、演習参加者の知識や経験がまちまちであることを示している。事前課題の小テストに解答した演習参加者の割合は、対面型で実施した前年度よりは増えていたが、小テストに取り組みないまま公開講座当日を迎えた演習参加者が 22 名中 10 名であったことも、この結果に影響していると考えられる。以上より、要件の「(7) 演習環境やコミュニケーションツールの事前習得」は解決できたが、「(1) 演習参加者間の差異の吸収」は解決できていなかった。また、「(2) 演習参加者のチームビルディング」は課題を残すこととなった。

公開講座当日の演習前半では、Slack を通じて演習参加者および聴講参加者に Zoom ミーティング情報を通知し、スムーズに開始することができた。演習後半に移る際のブレイクアウトルーム作成も、演習参加者を事前にブレイクアウトルームに割り当てる操作を済ませておくことでスムーズに進行できた。演習参加者と聴講参加者に対する、Zoom を用いた公開講座の進行に関するアンケート結果を表 5 に示す。トラブルがあっても解消して利用できたことが分かる。1 名のみ解消できないトラブルがあったと回答したものの、内容の記述欄には記載がなく詳細は把握で

表 4 事前課題のアンケート結果

Table 4 Questionnaire results on the pre-assignment.

	簡単	適切	難しい	わからない
事前課題の内容	4	10	8	0
	少ない・長い	適切	多い・短い	わからない
分量と期間	1	14	2	5

表5 Zoomに関するアンケート結果
Table 5 Questionnaire results on Zoom.

	満足	どちらとも 言えない	不満
Zoomでの進行	22	13	1
トラブル	特になし	あったが 解消した	解消できず
	23	12	1

きていない。以上より、要件の「(6) オンライン型での説明と進行」は解決できたと言える。

公開講座当日の演習後半のうち、演習参加者について述べる。前述のような知人同士のチーム、経験者やリーダーシップを発揮する参加者がいるチームでは、Zoomでの音声通話に加えてSlackでの文字ベース・スクリーンショットベースの情報共有を駆使してスムーズに作業を進めていた。一方で、セキュリティに関する初心者や、堅牢化の対象であるLinuxサーバに関する知識や経験が不足しているチームでは、どこから手を付ければよいか分からず戸惑っている様子もみられた。対面型の場合、こうしたチームからは何度も手が挙がり、会場内の運営スタッフが近くに待機して丁寧に手助けすることである程度の進捗が得られていた。オンライン型の場合、Slackによる学生サポートへの問い合わせや支援の依頼はスムーズに行われていたが、操作している様子を見ながら近くで見守るといった状況にはならないため、問題となっている箇所の情報がうまく伝わらず、サポートがスムーズに行えないケースもみられた。アンケートによると、演習への満足度は演習参加者の約64%が満足、約9%が不満という評価、学生サポートへの満足度は演習参加者の約64%が満足、不満は0%という評価であった(表6, 表7)。オンライン演習環境の満足度は高いが、1名のトラブルについては前述のZoom同様に詳細が不明である(表8)。また、Slackについても支障なく利用できていたと言える(表9)。以上より、要件の「(3) チーム内の円滑な作業」と「(4) 演習課題の実施中の問い合わせ」は解決できたと言えるが、問い合わせを問題解決に結びつけることは対面型よりも困難であった。

公開講座当日の演習後半のうち、聴講参加者について述べる。対面型では演習を統括する講師が演習参加者と聴講参加者の両方をケアする形態だったのに対して、オンライン型では聴講参加者への説明に集中する形とした。課題の具体的な内容や演習参加者の進捗状況を、説明資料や図2のダッシュボード、図5のチャートを利用しながら丁寧に説明した。また、一部のチームがSlackでやり取りしている内容をピックアップして紹介することで、臨場感のある解説になったと考えている。アンケートでは、回答者14名中8名となる約57%が満足と回答したが、対面型で実

表6 演習に関するアンケート結果
Table 6 Questionnaire results on the practice.

	簡単	適切	難しい	わからない
演習の内容	1	11	10	0

表7 学生スタッフに関するアンケート結果
Table 7 Questionnaire results on the supporting staff.

	満足	どちらとも 言えない	不満	わからない
学生スタッフの対応	14	5	0	3

表8 オンライン演習環境に関するアンケート結果
Table 8 Questionnaire results on the practice environment.

	満足	どちらとも 言えない	不満
利用しやすさ	15	7	0
トラブル	特になし	あったが 解消した	解消できず
	13	8	1

表9 Slackに関するアンケート結果
Table 9 Questionnaire results on Slack.

	満足	どちらとも 言えない	不満
利用しやすさ	13	9	0
トラブル	特になし	あったが 解消した	解消できず
	19	3	0

施した2019年度の9名中4名となる約44%より改善している。以上より、要件の「(5) 聴講参加者が演習の状況を把握」は解決できたと言える。

5.2 オンライン演習環境の運用

オンライン型での実施が初めてだったことから、オンライン演習環境のサーバおよびネットワークには余裕のあるリソースを配分した。結果として、事前課題から公開講座の終了まで、特に大きな負荷がかかることはなく、障害の発生も観測されなかった。また、演習参加者からのアクセス遅延や障害の報告も演習中は発生しなかった^{*3}。

ネットワークトラフィックは演習後半で各回線ごとに10 Mbps程度であったことから、完全な二重化ではなく1台に集約して、やや小規模な予備環境を準備するactive-standby構成も考えられる。しかしながら、我々が運営する公開講座は授業や連続講座のような複数回の実施で

^{*3} 前述のとおり、アンケートでは1名が解消できない不具合を報告しているが、運営スタッフ側では認知できていない。

はなく当日1回のみであり、実質的な演習の時間が90分強という短時間で実施している。このため、障害時に迅速なりカバーを行う観点から、今回のような active-active 構成のほうが適切であると考えている。

演習参加者が使用する VM のライブマイグレーションはできたほうがよいが、サーバ間で共有するストレージを配置する必要がある。VM に障害が発生する前までの到達度はダッシュボードサーバに記録されているので、チームごとの到達度確認やスコアの集計という観点では、障害発生時の集計手順さえ検討できていれば、VM は今回のように cold standby 方式でも問題ないと考えられる。

5.3 オンライン演習環境の割り当て方法

演習環境をチームで共有せず1人1台の設計としたことについては、アンケートの自由記述欄に「VMware の仮想マシンが一人一台つかえるのもよかったです」という趣旨の回答が複数あった（原文のまま）。

一方で、ダッシュボードサーバの集計方法については、Slack で「同じことをなぜ3人に1回ずつやらせるのかというのは多少疑問に思いましたが、演習自体は非常に楽しめたので満足です」というコメントが1件あった（原文のまま）。ダッシュボードサーバ上でチーム全体の修正状況をマージすれば、他のメンバーが同じ脆弱性を修正する必要はなくなるが、演習環境ごと（チームのメンバーごと）の集計としたのは単に高得点を目指すだけではなく、修正方法をチーム内で共有し理解してもらうことを意図したものである。今後、同様の集計方法を採用する場合は、演習参加者に適切に意図を伝えるよう留意する。

5.4 公開講座の運営

公開講座全体の運営として大きな問題はなかったが、対面型では起きなかった、あるいは解消できていた点を2つ挙げる。

第1は、申し込み後のキャンセル（無断を含む）が多かったことである。オンライン型で無償のために申し込みやすい反面、気軽にキャンセルできてしまう点は、場所の制約なく参加できる利点の裏返しと言える。対面型では、当日に聴講参加者から希望者を募って演習参加者の欠員を埋めていたが、オンライン型では事前課題を通じてオンライン演習環境等に習熟する必要があったため、欠員補充は見送らざるを得なかった。また、所属する高校に設置されている PC から接続する予定だったが、コンテンツフィルタリングによって接続できないことが公開講座の2日前に発覚して、キャンセルに至った事例もあった。これについては、今後は募集要項で事前の接続確認を早めに行うよう依頼することで解決すると考えられる。

第2は、演習参加者の熱気や活気がオンラインでは感じられないことである。2019年度の実施[4]では、模擬的な

サイバー攻撃に成功すると鉄道模型の動作を制御できる課題にしたため、参加者同士の熱気にも拍車がかかった印象がある。Slack でのコミュニケーションを部分的に取り上げることができたが、図2のダッシュボード等には現れない演習参加者の活動を横断的に可視化する方法は今後の課題と言える。

5.5 コミュニケーションツールの選定

事前課題を実施するうえで、Zoom のような同期型のツールではなく、非同期型のメッセージングが必要であると考え、Slack を選定した。しかし、公開講座の設計段階では、大学生以下、特に高校生には Slack のハードルが高いのではないかという懸念が挙げられていた。

代替手段として考えられるものに、LINE がある。高校生にもなじみ深いものと言えるが、スレッドやメンションといった機能がないと学生スタッフによるスムーズな状況把握と支援が難しいと考え、採用を見送った。

こうしたツールは年々、新サービスや新機能により発展するものであり、今後も継続した比較検討が必要であると考えている。

6. 関連研究

村山[5]は、高等学校における科目「情報セキュリティ」の授業実践について報告している。サイバー攻撃に関する具体的な題材に IPA が提供する AppGoat^{*4} を利用するなどして、実践的な演習に取り組んでいる。AppGoat の教材は改訂の頻度が高くないが、実際のサイバー攻撃では基本的な対策の不足を突く攻撃が多いため、複数のクラスや年度で取り組む教材としては適切であると言える。我々の運営する公開講座でも基本的な題材を軸に据えつつ、IoT 機器への攻撃やインターネット通販の増加といったトピックと組み合わせて、参加者が興味を持つ内容とすることを心がけている。

阿部ら[6]は、入門者向け大会イベントとしての CTF 実施と、余興としてのアドベンチャー型ゲームと組み合わせた運営を提案している。CTF では、参加者の知識や技能に応じて課題を設定し、チームで取り組む形式となっている。観戦者は余興ゲームを通じて CTF 参加チームを応援することができ、CTF 参加者と観戦者が協力してイベントに取り組む。我々の運営する公開講座では、CTF 参加者が演習参加者に、観戦者が聴講参加者に対応している。本稿で述べたオンライン型では、聴講参加者は演習参加者の動向を、講師の説明を通じて理解できるが、演習参加者はその状況を把握していない。公開講座という運営形態から、聴講参加者には解説を行うことを重視しており、演習参加者に積極的に関与することは想定していなかつ

^{*4} <https://www.ipa.go.jp/security/vuln/appgoat/>

た。イベントとしての一体感や盛り上がりを演出する一助となる可能性はあり、今後検討を行う。

サイバーセキュリティの演習環境はサイバーレンジとも呼ばれ、サイバーセキュリティ教育ではこれを柔軟かつ高速に準備することが重要である。中田ら [7] は、複数の演習コンテンツを動作させる基盤環境を提案している。演習を行う利用者の PC 上に VM として Ubuntu を動作させ、Docker コンテナを利用して複数の端末やサーバ、ルータを起動する。演習シナリオとして OWASP が提供する WebGoat^{*5} の教材を移植したり、独自の演習シナリオを構築することができる。我々の公開講座では、対面型ではこちらで用意した演習参加者用ノート PC に VM を導入して必要な演習環境を構築していたが、コンテナによる複数ホスト等の動作は行わず、会場内に別途設置するサーバと組み合わせる構成を取っていた。演習参加者の進捗状況をサーバ上で一括管理することも想定した構成であり、授業として実施する場合と、一種のコンテスト的なイベントとして単発で実施する場合の要件の違いと言える。

寺嶋ら [8] は、演習企画者がクラウド上にサイバーレンジを構築する際の、構築手順や記述するファイルの内容を削減するための仕組みを提案している。演習参加者はサイバーレンジの構築過程で作成される VPN 認証ファイルを受け取り、複数のホストやサブネットからなる演習環境に接続して演習を行う。演習環境をネットワークを介して提供するという点は本研究と類似するが、本研究では単一ホストの堅牢化を扱ったこと、GUI を含むデスクトップを提供するほうが利用者に分かりやすいと考えて Web ブラウザによる RDP 方式を採用したことが異なる。

村木ら [9] は、大学の授業間といった短時間に演習環境を切り換えるため VM のクローン機能を使用しているが、これにかかる時間を ZFS クローンにより短縮する方法を提案している。本研究でも多数の演習参加者のために同一の環境を提供する必要があり、雛形となる VM の仮想ディスクを VMware ESXi のリンククローンで展開した。我々の運営する公開講座では先行研究より準備に時間がかげられることから、ハイパーバイザの標準的なファイルシステムとクローニング機能で十分な速度が得られている。我々の公開講座は年 1 回の実施であり、特定の構成に依存しないほうが安定した運用に寄与すると考えている。

Debatty ら [10] は、VM により構築した演習環境に Web ブラウザを用いて接続する形式での実装を提案している。ハイパーバイザとして VirtualBox を、演習環境のデスクトップへのアクセスには Web ブラウザで動作する Apache Guacamole^{*6} を採用している点が異なる。本研究

ではハイパーバイザとアクセス方法のいずれも VMware ESXi で実装することで、リモートデスクトップ用のゲートウェイを別途用意する必要がなく、より単純な構成を実現したと言える。

7. まとめと課題

本稿では、実践的な演習を伴うオンライン公開講座として、サイバーセキュリティ堅牢化演習を実施するにあたり、満たすべき要件を整理するとともに具体的な解決策を述べた。また、それらの解決策で要件がどの程度解決できたかについて、実際に公開講座を運営した経験に基づく評価と考察を述べた。

今後の課題として、チームビルディングにおけるファシリテーターの役割を担うスタッフの追加、演習参加者のキャンセル分を補充する可能性、結果に表れないチーム内コミュニケーションの横断的な可視化と聴講参加者の関与、演習参加者間の差異の吸収と当日の支援について検討が必要なことを述べた。特に最後の点については、演習参加者は様々な動機を持っており、事前課題への取り組み方もまちまちであるため、当日の支援と組み合わせる改善を検討する必要があると考えている。具体的には、オンライン型では対面型と同等の支援が難しいことから、これまでは特に求めなかった、Linux コマンドの使用やネットワークの基礎知識を参加募集の際に明記することが考えられる。

2021 年度も引き続きオンライン型のみでの実施を計画しているが、対面型の再開が可能となった場合にも、オンライン参加と組み合わせるハイブリッド型の開催について検討していきたい。

謝辞 公開講座の教材や演習環境の整備に協力してくれたストーンビートセキュリティ (株) の関係者、広報面で支援してくれた McAfee Enterprise の関係者、参加者からの質問に丁寧に対応してくれた明星大学情報学部の学生スタッフに感謝します。

参考文献

- [1] 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 2021 (2021).
- [2] SECCON: SECURITY CONTEST OFFICIAL SITE, SECCON (online), available from <<https://www.seccon.jp/>> (accessed 2021-11-08).
- [3] picoCTF: picoCTF - CMU Cybersecurity Competition, Carnegie Mellon University (online), available from <<https://picoctf.org/>> (accessed 2021-11-08).
- [4] 丸山一貴, 佐々木伸彦, 高谷宏幸: ペタ語義: 実践的演習を伴うサイバーセキュリティ公開講座の取り組み, 情報処理, Vol.61, No.6, pp.628-631 (2020).
- [5] 村山佳之: 科目「情報セキュリティ」の授業実践, 情報処理, Vol.62, No.1, pp.14-19 (2021).
- [6] 阿部隆幸, 中矢 誠, 楠目 幹, 富永浩之: 初心者向けのハッキング競技 CTF による情報リテラシーとセキュリティ

^{*5} <https://owasp.org/www-project-webgoat/>

^{*6} <https://guacamole.apache.org/>

ティの導入教育のためのオープンな大会イベント-高大連携に向けたクイズ形式のアドベンチャー型の余興ゲームの試作と予備実験-, 信学技報, Vol.IEICE-116, No. IEICE-ET-517, pp.123-128 (2017).

- [7] 中田亮太郎, 慎 祥揆, 笠井洋輔, 豊田真一, 瀬戸洋一: 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, 情報処理学会デジタルプラクティス, Vol.11, No.2, pp.414-433 (2020).
- [8] 寺嶋友哉, 仲山昌宏, 横山輝明, 小出 洋: KAKOI: クラウドを利用したサイバーレンジをシンプルかつ安全に構築する新しいツール, 情報処理学会研究報告, Vol.2021-CSEC-93, No.15, pp.1-9 (2021).
- [9] 村木優太, 上原哲太郎: サイバーレンジ演習環境展開の高速化手法, 情報処理学会研究報告, Vol.2018-CSEC-83, No.1, pp.1-7 (2018).
- [10] Debatty, T. and Mees, W.: Building a Cyber Range for training CyberDefense Situation Awareness, *Proceedings of the International Conference on Military Communications and Information Systems (ICMCIS)*, pp.1-6 (2019).



末田 欣子 (正会員)

1995年 東京電機大学大学院博士前期課程修了。同年日本電信電話株式会社 入社。以来、ネットワークソフトウェア、ネットワーク基盤技術の研究に従事。2018年より明星大学情報学部にて、初学者プログラミング教育、IoT 関連ネットワーク技術や情報セキュリティ研究に従事。博士 (工学)。電子情報通信学会, IEEE 各会員。



丸山 一貴 (正会員)

1999年東京大学工学部機械情報工学科卒業, 2001年同大学大学院工学系研究科情報工学専攻修士課程修了, 2004年同情報理工学系研究科知能機械情報学専攻博士課程修了。電気通信大学情報基盤センター助教, 東京大学情報基盤センター助教等を経て, 2013年明星大学情報学部情報学科准教授, 2022年教授, 現在に至る。プログラム開発環境やユーザインタフェースの研究, 大学におけるICTサービスの設計と運用に従事。博士 (情報理工学)。日本ソフトウェア科学会, ACM, IEEE 各会員。



佐々木 伸彦

2015年にストーンビートセキュリティを設立, 代表取締役。2016年から外務省最高情報セキュリティ責任者 (CISO) 補佐官を務める。脆弱性診断や情報セキュリティコンサルティング, トレーニング講師など幅広く活躍中。CISSP, CISA, GCFA, LPIC-3 Security。



高谷 宏幸

Trellix プロフェッショナルサービス本部のシニアトレーナーとして研修サービスに従事。Trellix および Skyhigh Security が提供するセキュリティ対策製品, インシデント対応等の研修を官公庁や企業向けに実施している。CISSP, CISA。