情報処理学会論文誌　教育とコンピュータ　Vol.5　No.2　20–29 (June 2019)

論　文

大学学部生を対象とするセキュリティ教育における サーバ侵入演習の実践と評価

鈴木 大助[1,a)]

受付日 2018年8月18日，再受付日 2019年1月9日，
採録日 2019年3月11日

概要：本研究の目的は，大学学部の専門課程における情報セキュリティ教育の一環として，脆弱性を利用したサーバ侵入を体験する演習を提案・実践し，その教育効果を明らかにすることである．演習では，各自が管理するノート PC の上に実験のための仮想環境を設けサーバ攻撃実験を行う．また，受講生自身が実験室内に構築したサーバへの攻撃実験とセキュリティ関連法規の学習も行う．一般的には大学院で実施される攻撃実践演習であるが，カリキュラムの工夫によって，学部であっても十分実施可能となった．演習の前後で，授業到達目標に関する自己評価および理解度確認テストを実施したところ，本演習がセキュリティ分野の知識向上に効果があることが分かった．また，受講生のコメントからは，法令遵守について学ぶ機会が学んだ技術を悪用させない抑止力となりうることが示唆された．

キーワード：情報セキュリティ教育，ペネトレーションテスト，倫理的ハッキング，カリキュラム設計

Practice and Evaluation of a Penetration Testing Exercise in Security Education for Undergraduate Students

Daisuke Suzuki[1,a)]

Received: August 18, 2018, Revised: January 9, 2019,
Accepted: March 11, 2019

Abstract: The aim of this study is to propose and practice an exercise to experience server intrusion using vulnerability as a part of information security education in the specialized course of undergraduate department, and to clarify the educational effect. In the exercise, students perform server attack experiments in virtual environments on their laptops and also experience attacks on servers in their laboratory. In order to participate in this class, students are required to learn about compliance. This kind of exercise is generally carried out at the graduate school, however, by devising a curriculum, it is possible for undergraduates to implement this type of exercise. Student self-assessment and confirmation test clarified that this exercise is effective for students to acquire security knowledge and skills. Students' comments, moreover, indicate that compliance training is possible to have the effect of preventing students from abusing skills acquired in the exercise.

Keywords: Information security education, penetration testing, ethical hacking, curriculum design

1. はじめに

多くの組織が各種情報をネットワークにつながれたコンピュータ上に保有・管理し，ネットワーク経由で利用している昨今，情報資産を脅威から守るため，組織に関わるすべての人間に対して情報セキュリティ教育を行うことが求められている．大学においては，これから社会組織に人材を送り出す教育機関として，文系・理系を問わず情報セキュリティ教育を行う必要がある．

情報資産を脅かすサイバー攻撃は，簡単なものであれば，少しその方法を学んだり，巷に溢れているツールを用いたりすることで，その気さえあれば誰でも実行できる．情報システムやネットワークを利用するすべての人は，その現

[1] 北陸大学
Hokuriku University, Kanazawa, Ishikawa 920–1180, Japan
[a)] d-suzuki@hokuriku-u.ac.jp

実を知らなければならない．そのため，情報セキュリティ教育の一環としてサイバー攻撃の攻撃者となる体験をし，いかに攻撃を実行しうるかを学ぶことが重要である．

これまでのところ，セキュリティ教育においてサイバー攻撃手法を実践する演習を実施することは，日本では主に情報系の大学院に限られており [1], [2]，大学学部においては，たとえ情報系の専門情報教育であっても，一般的ではない．

しかし，実際の攻撃手法や攻撃者の行動を知ることはセキュリティにおいて重要である．そもそも，攻撃者がいるからこそ，防御の必要性が生じる．具体的な攻撃についてよく知らない状態では，防御の知識や技術を積極的に学ぼうとは思わないのではないだろうか．このため，攻撃者となる体験を通じて，サイバー攻撃に対する認知を高めることが必要であると考える．はたして，大学学部において攻撃手法を取り入れた演習を実践することは可能であろうか．また，その効果はどのようなものであろうか．

本研究の目的は，サイバー攻撃実践演習を学部の専門情報教育の一環として実施可能な形で提案・実践し，その教育効果を明らかにすることである．

攻撃手法を取り入れた演習を大学学部生向けに実施するにあたっては 2 つの問題点がある．第 1 に，未成熟な学部生を対象に攻撃技術を教えることで，技術の悪用等の弊害が生じるのではないかと懸念されている点 [3] である．第 2 に，サイバー攻撃演習は一般的には大学院レベルの応用的な内容であり，前提とする基礎知識・技術が少なくないため，科目配置や演習の難易度に配慮が必要な点である．

本研究では，主に大学院生を対象として実施されている攻撃実践演習を参考にしながら，学部生を対象として実施可能とするために演習内容や科目配置等のカリキュラムを設計し，また，攻撃技術の悪用に対する懸念を解消するためにコンプライアンス教育をあわせて実施する設計とした．

まず，攻撃手法を実践する機会としてのサーバ侵入演習授業のカリキュラム設計，評価設計および事前評価を行った [4]．続いて，筆者の担当する情報専門コースの大学 3 年生を対象とする授業においてサーバ侵入演習授業を実践し，到達目標に関する自己評価および理解度確認テストを事前事後で実施したところ，その効果が確認された [5]．本稿は，この実践について詳述し，検討報告するものである．

2. 関連研究

セキュリティ教育において具体的な攻撃手法を取り扱うことについては，海外で先行してさまざまな提案や議論がなされている．

Yang らは情報セキュリティ教育にハッキング技術を組み込む提案と大学院生を対象とした実践について報告している [6]．

Mateti は，隔離された LAN において実際に各種攻撃を実行する機会を含む大学 4 年生を対象としたセキュリティ教育コースを提案している [7]．

Trabelsi らは，大学学部上級向けのセキュリティ教育コースで，具体的な DoS 攻撃の方法を学ぶ機会を提供したところ，多くの学生が演習に満足し DoS 攻撃の理論的概念の理解が深まったと回答する一方で，また多くの学生が実験環境外において興味本位で DoS 攻撃を実行してしまっていたことを報告している [8]．

Harris は，精神的に未熟である大学生を対象にサイバー攻撃の具体的手法を教えることの倫理的問題についてかねてより指摘している [3]．

日本では，大学学部生を対象とするセキュリティ教育において攻撃手法を実践する機会を設けることは今のところ一般的ではない．

立岩らは学生に攻撃技術を教えるべきではないという前提に立ち，仮想マシンからなる仮想的なネットワーク上に，攻撃を実行する仮想クラッカーを設けて受講生が防衛の学習に専念できるシステムを開発している [9]．

福山らは仮想マシンネットワークにおいて攻撃手法の学習も取り扱っているが，Cisco ネットワーキングアカデミー修了生を対象とする評価実験は行われているものの，大学学部の実際の授業での実践報告はなされていない [10]．

八木らは，早稲田大学において産学連携によるサイバーセキュリティ教育を実施しているが，攻撃手法を実践する演習は大学院生が対象であり，大学学部生に対しては講義がメインである [1]．

後藤らは大学間連携による協働開講によって，実践セキュリティ人材育成コースを実施しており，その中には攻撃者の視点から脆弱性検査を行う演習を実施する授業も含まれているが，その対象は大学院生である [2]．

以上のように，日本の大学において学部生を対象とするセキュリティ教育の一環として攻撃実践演習を実施することは今のところ一般的ではない．また，海外の事例では攻撃手法を教育することの有用性についての報告がある一方で，具体的な弊害や倫理的な問題も指摘されている．

本研究では，演習内容や関連科目の配置も含めてカリキュラムを設計し，攻撃技術の悪用に対する懸念を解消するためにコンプライアンス教育をあわせて実施する科目設計とすることで，学部生を対象とした攻撃実践演習を問題なく実施することを可能とした．次章では，カリキュラムの全体像とサーバ侵入演習の詳細について説明する．

3. 科目の全体像とサーバ侵入演習

3.1 科目の全体像と関連科目

攻撃手法を実践する機会としてのサーバ侵入演習は北陸大学未来創造学部 3 年後期科目「システム管理 II」の一部として行った．2017 年度の授業日程を**表 1** に示す．

「システム管理 II」は各種 Linux サーバの構築と脆弱性

表 1　「システム管理 II」授業日程
Table 1　"System Management II" lecture schedule.

授業回	授業内容
1	イントロダクション／事前評価
2	サーバのネットワーク設定
3, 4	DNS サーバ構築
5, 6	WEB サーバ構築
7, 8	メールサーバ構築
9	ファイル共有サーバ構築
10	セキュリティ（アクセス制御・パケットフィルタ）
11	実験用仮想環境の構築
12	仮想環境でのペネトレーションテスト
13	情報倫理・コンプライアンス／誓約書提出
14	実験室内でのペネトレーションテスト
15	事後評価

を利用したサーバ侵入等の攻撃を行う体験を通じて，① 各種 Linux サーバ構築能力の習得，および，② サーバに対する攻撃の存在を知り，セキュリティ分野の知識習得の契機とすること，を目的とする授業である．

第 1 回から第 9 回まではサーバ実機（Dell PowerEdge T110 II）上に CentOS 6.8 をインストールし，これを利用した各種サーバ構築を実践する．第 10 回にはサーバのセキュリティのうち特に TCP Wrapper を利用したアクセス制御や iptables を利用したパケットフィルタリングについて学び，構築したサーバに適用する．その後，第 11 回から第 14 回の 4 回でサーバ侵入演習を実施する．サーバ侵入演習の詳細については 3.2 節以降において詳述する．

受講生は日本語と IT 専門学習のために中国から来た編入留学生 3 年生 17 人で，受講段階では，日本語能力は日本語能力試験 2 級レベルである．受講生は編入前にはネットワークや Linux サーバ構築・管理の学習を十分に行っていないことが分かっている．このため，「システム管理 II」の前提科目として，3 年生前期には「ネットワーク論 I」「システム管理 I」をそれぞれ置き，その中で基礎となる知識・技術の学習を行っている．

「ネットワーク論 I」では TCP/IP ネットワークの基礎概念の学習とルータ・スイッチを用いたネットワーク構築の実践を行っている．「システム管理 I」では，受講生は大学から貸与された Windows ノート PC に VirtualBox を利用して仮想環境を構築し，Ubuntu および CentOS をゲスト OS としてインストールし，Linux の学習・各種コマンドの実習を行っている．これらの科目が前提として存在することで，「システム管理 II」の授業においてサーバ構築実習とサーバ侵入演習の実践が可能となっている．

また，「システム管理 II」の発展科目として，4 年生前期に「情報セキュリティ論」を置いており，情報セキュリティの基本的な理論と技術の学習，および，システム開発・

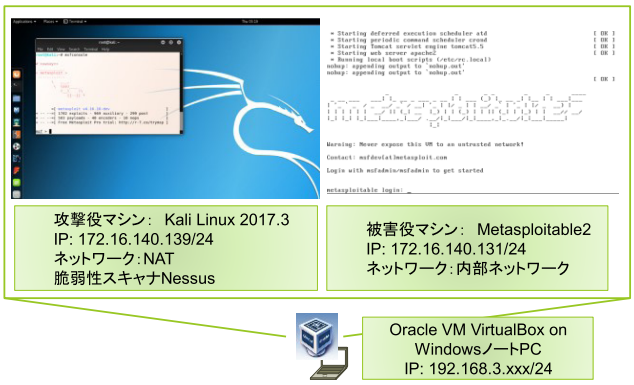

図 1　実験用仮想環境
Fig. 1　Virtual laboratory for penetration testing.

システム運用において必要とされる実践的な技術の学習を行っている．本稿で提案しているサーバ侵入演習はその学習の前段階として情報セキュリティ分野に対する興味を喚起することを狙いの 1 つとしている．

3.2　サーバ侵入演習の目的と概要

サーバ侵入演習は，脆弱性を利用したサーバ侵入等の攻撃を行う体験を通じて，攻撃者の行動を知り，セキュリティ分野の知識習得の契機とすることを目的とする．90 分を 1 回として，4 回の演習からなる授業構成とした．

1. 実験用仮想環境の構築
2. 仮想環境でのペネトレーションテスト
3. 情報倫理・コンプライアンス/誓約書提出
4. 実機サーバに対するペネトレーションテスト

次節以降，各回の授業内容について説明する．

3.3　実験用仮想環境の構築

1 コマ目は実験用仮想環境の構築を実施する．サーバ侵入演習では攻撃役マシンと脆弱性を持った被害役マシンを用意するが，脆弱性を持ったマシンは外部ネットワーク環境から切り離した環境で扱う必要がある．そこで，実験用仮想環境を構築し，そのうえで実験を行うこととした．構築する実験用仮想環境の模式図を**図 1** に示す．

受講生は大学から貸与されているノート PC（Dell Vostro 15 3000/Windows 8.1 および Windows 10 が混在）に仮想化ソフト（Oracle VM VirtualBox [11]）をインストールし，ゲスト OS として攻撃役マシン（Kali Linux 2017.3 [12]）と被害役マシン（Metasploitable2 [13]）を導入する．被害役マシンはホスト OS との通信も行わないためネットワーク設定は内部ネットワークとし，攻撃役マシンのネットワーク設定は NAT とする．攻撃役マシンと被害役マシンは同一のネットワークに所属するよう IP アドレスを設定する．例では，攻撃役マシンを 172.16.140.139/24，被害役マシンを 172.16.140.131/24 としている．なお，ホスト OS である Windows の IP アドレスはノート PC の設置された環

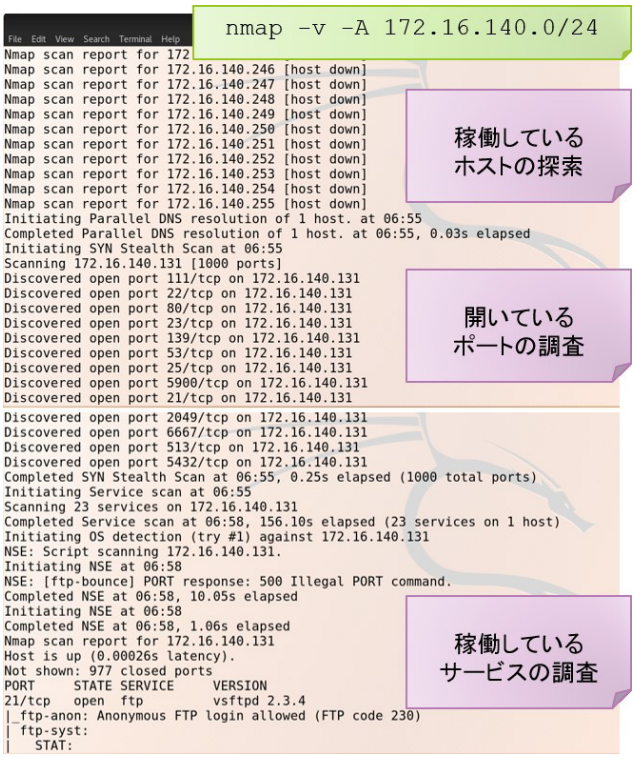

図 2　ポートスキャンの実行例

Fig. 2　Port scanning using Nmap.

境に応じて決定する．例では，192.168.3.xxx/24 としている．また，次回以降で利用するため，攻撃役マシンに脆弱性スキャナ Nessus [14] をインストール・設定する作業を実施する．

3.4　仮想環境でのペネトレーションテスト

2 コマ目は，1 コマ目に構築した実験用仮想環境においてペネトレーションテストを実施する．

まず，攻撃役マシンから被害役マシンに対してポートスキャン（Nmap [15]）を実行し，攻撃対象の選定，開いているポートや稼働しているサービスの調査を行う．攻撃役マシンである Kali Linux の端末上で “`nmap -v -A 172.16.140.0/24`” を実行した場合の画面の一部を**図 2** に示す．

探索対象であるネットワーク上で稼働しているホストとして 172.16.140.131 が発見され，続いて当該ホストで開いているポートとして 111, 22, 80, ··· と次々に検出されている．さらに，稼働しているサービスの調査結果として 21 番ポートで vsftpd 2.3.4 が稼働していることが見てとれる．

次に Nessus を利用して攻撃対象の脆弱性検査を実施する．Kali Linux にインストールした Nessus を起動し，ブラウザで https://127.0.0.1:8834 を指定，“New Scan”，“Basic Network Scan” を選択する．Targets に攻撃対象ホストの IP アドレスとして，ここでは先のポートスキャンで発見された Metasploitable2 の IP アドレスである 172.16.140.131 を設定し，検査を開始する．Metasploitable2 を対象として

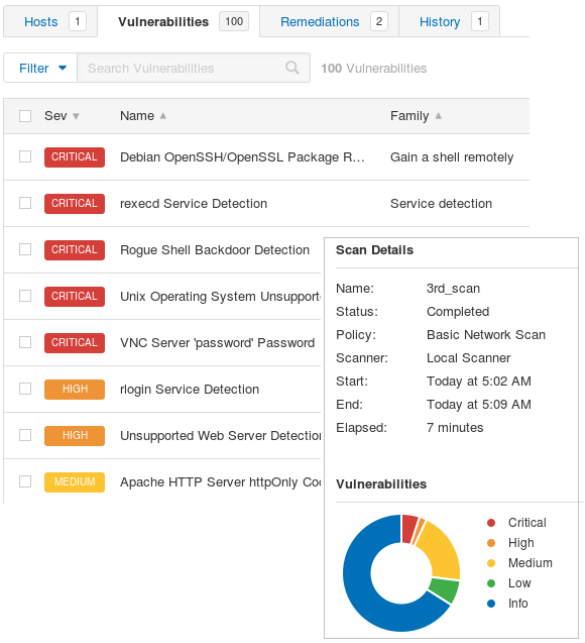

図 3　Metasploitable2 を対象とした Nessus を利用した脆弱性検査の実行例

Fig. 3　Vulnerability assessment on Metasploitable2 using Nessus.

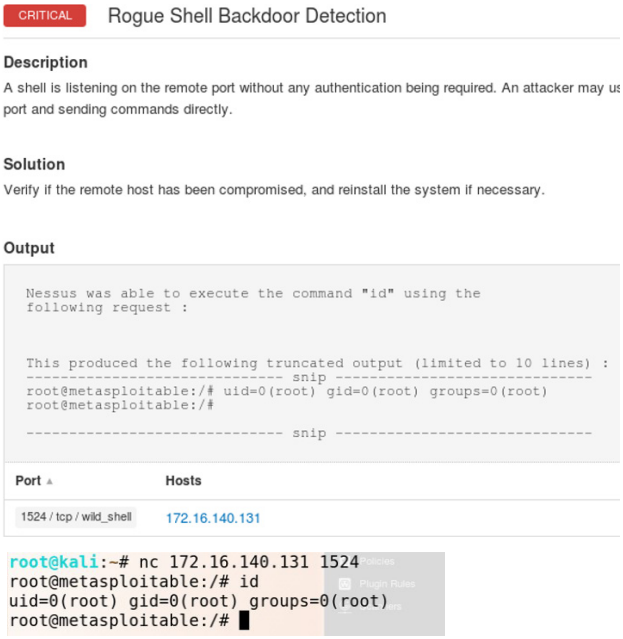

図 4　Rogue Shell Backdoor Detection の脆弱性利用攻撃

Fig. 4　Details of “Rogue Shell Backdoor Detection” and backdoor command execution with Netcat.

Nessus を利用して脆弱性検査を実行した結果の例を**図 3** に示す．

100 個の脆弱性が発見され，Critical から Info までレベル分けされて表示されている．Critical の上から 3 つ目に “Rogue Shell Backdoor Detection” が確認できるため，当該脆弱性を利用した攻撃を試みる．当該脆弱性の詳細画面と，当該脆弱性利用攻撃を**図 4** に示す．

“Rogue Shell Backdoor Detection” の詳細画面によると，172.16.140.131 の 1524 番ポートに認証なしで直接コマンドを送信できることが読み取れる．そこで，ネットワークユーティリティの 1 つである Netcat [16] を利用して “`nc 172.16.140.131 1524`” を実行することで root 権限の奪取が完了する．以上がサーバ侵入の一例である．

別の例として，vsftpd 2.3.4 にもバックドアが仕込まれているため，この脆弱性を利用したサーバ侵入も可能である．ここではツールとして Metasploit framework [17] を利用する．Kali Linux の端末上で “`msfconsole`” を実行すると Metasploit framework のコンソールが起動する．コンソールで入力するコマンドの例と実行結果を**図 5** に示す．

“`search vsftpd`” で vsftpd に関する脆弱性を検索し，“`use exploit/unix/ftp/vsfpd_234_backdoor`” で当該脆弱性利用を指定，“`set rhost 172.16.140.131`” で攻撃対象を設定し，“`run`” で攻撃を実行する．vsftpd 2.3.4 の脆弱性利用攻撃によって，正当な権限を持たない者でも被害役ホストである Metasploitable2 上で任意のコマンドが実行可能になっていることが確認できる．以上が仮想実験環境における Metasploitable2 を対象とした脆弱性利用攻撃の一連の流れである．受講生は各自の PC においてこの一連の流れを体験する．

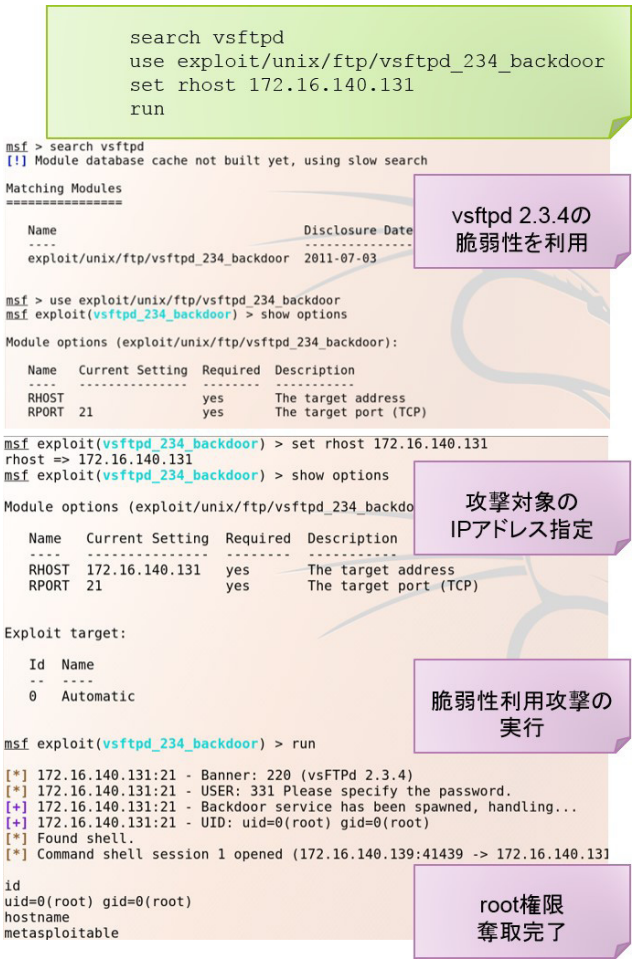

図 5　vsftpd 2.3.4 の脆弱性を利用した攻撃の実行例

Fig. 5　VSFTPD 2.3.4 backdoor command execution with Metasploit framework.

3.5　情報倫理・コンプライアンス/誓約書提出

3 コマ目は，情報倫理・コンプライアンスについて学ぶ．本演習自体は実験室環境においてのみ行うが，受講生は実験室環境においてサーバ侵入実験を行っているうちに，現実に社会で稼働しているサーバを対象に侵入を試みたくなる誘惑に駆られる可能性がある．精神的に未熟である大学生に攻撃技術を教える場合の倫理的問題について Harris が指摘している [3]．こうした点をふまえ，サイバー犯罪関連法規について学び，技術を悪用しないこと，悪用した場合にどのような罰があるか学ぶ機会を設けることとした．

おそらくほとんどの大学において入学時にネットワーク利用ガイダンスや情報倫理教育を実施していると思われる．筆者の所属大学においても入学時にネットワーク利用ガイダンスの受講を必須としており，インターネットにおける軽率な行為がどのような事件を招きうるかといったことや情報セキュリティ関連の法令と犯罪事例について学習している [18]．しかし，サーバ侵入演習という特殊な演習実施にあたっては，法令遵守の意識がより強く求められる．そこであらためて情報倫理・コンプライアンスについて学習する機会を設けた．

本時の演習では，課題として，自分が管理していないサーバに対して侵入や攻撃を行った場合，日本の法律ではどのような罪に問われるか調べて報告するよう求めた．その際，本学入学生を対象に行う情報ガイダンス [18] で説明用に用いているスライド資料を提供し，必要に応じて参照するよう伝えた．また，情報セキュリティ関連の法律の学習に資するため，総務省の国民のための情報セキュリティサイト [19] を案内した．提出された報告の一部を**図 6** に示す．不正アクセス禁止法と不正指令電磁的記録作成等の罪に該当すると報告されている．さらに，本学所定の誓約書に署名のうえ，提出するよう求めた．

なお，本演習の受講生は中国からの留学生であり，日本

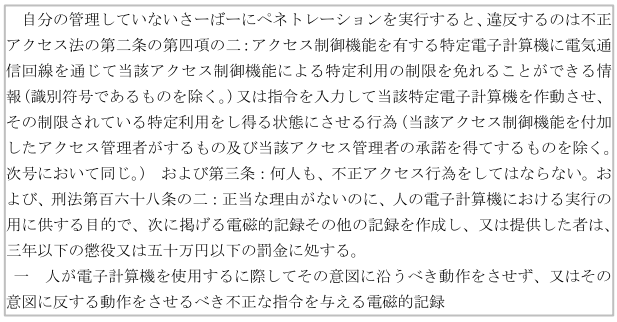
自分の管理していないさーばーにペネトレーションを実行すると、違反するのは不正アクセス法の第二条の第四項の二：アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）　および第三条：何人も、不正アクセス行為をしてはならない。および、刑法第百六十八条の二：正当な理由がないのに、人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、三年以下の懲役又は五十万円以下の罰金に処する。
一　人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録

図 6　該当する罪に関する受講生による報告例（一部）

Fig. 6　Laws in Japan related to penetration testing reported by a student.

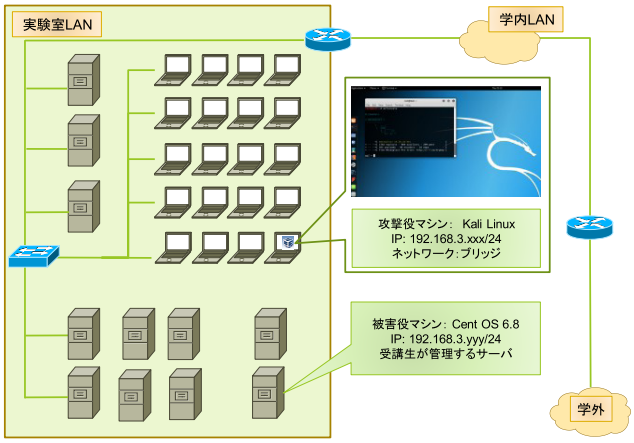

図 7　実機サーバに対するペネトレーションテストを実行する実験室環境

Fig. 7　Real laboratory for conducting penetration testing on real servers.

の法律について学ぶ機会や学んだ経験はきわめて少ない．本時の演習において，サイバー攻撃に関連する日本の法律について自分で調べて報告し，その内容をふまえて誓約書に署名・提出することが，学んだ攻撃技術の悪用を防ぐ効果をもたらすと期待される．

また，本時に限らず，演習全体を通じてことあるごとに，自分の管理するコンピュータ以外にペネトレーションテストをしかけることが犯罪となりうることを配布スライド等に明記し強調した．

3.6　実機サーバに対するペネトレーションテスト

4 コマ目は実験室環境内において実機サーバに対するペネトレーションテストを実行する．実験室環境を**図 7** に示す．

実験室にはサーバ構築演習において受講生が各自で構築したサーバが設置されている．本時は，この各自が管理する実験用サーバに対してペネトレーションテストを実施する．一般的に攻撃実践演習は，安全面の配慮から仮想環境で実践することが多い．しかし，実機サーバに対して攻撃を行う体験の機会があれば，よりサイバー攻撃に関するイメージがわきやすいと考える．「システム管理 II」では，前半の授業で受講生自身が 1 人 1 台サーバを構築し，その管理を各自で行っているため，各受講生が各自の管理下にあるサーバへの攻撃を実施することができる．この授業設計により，実機への攻撃体験の機会を提供することが可能となっている．

被害役となるサーバは実験室 LAN である 192.168.3.0/24 に所属しており，その OS は CentOS 6.8 である．攻撃役マシンは引き続き Kali Linux を用いるが，ゲスト OS としてのネットワーク設定をブリッジとし，被害役サーバと同じネットワークに所属させる．この環境の下で，受講生は 3.4 節と同様のペネトレーションテストの手順を実行し，

表 2　自己評価質問項目

Table 2　Self-assessment questions.

項目名	質問内容
1. Linuxインストール	LinuxをPCやサーバ機にインストールできる。
2. 仮想環境	VirtualBox等の仮想化ソフトを利用して複数のLinuxをゲストOSとして使用する環境を構築できる。
3. 基本コマンド	Linuxの基本的なコマンドについてマニュアルを見ずに使うことができる。
4. 各種コマンド	使い方を知らないLinuxコマンドについてマニュアルを調べながら使うことができる。
5. ネットワーク設定	Linux機について環境に応じたネットワーク設定（固定IPアドレスの設定等）ができる。
6. DNSサーバ構築	DNSサーバの構築ができる。
7. WEBサーバ構築	WEBサーバの構築ができる。
8. メールサーバ構築	メールサーバの構築ができる。
9. ファイルサーバ構築	ファイル共有サーバの構築ができる。
10. パケットフィルタ	iptables等を利用してパケットフィルタリングができる。
11. ポートスキャン	nmap等を利用してターゲットの開いているポートやOSの調査ができる。
12. 脆弱性検査	Nessus等を利用してターゲットの脆弱性検査ができる。
13. 脆弱性利用攻撃	Metasploit Frameworkを利用して脆弱性を持ったターゲット（Metasploitable）に侵入できる。

脆弱性検査や脆弱性利用攻撃を試み，その結果について報告する．

以上がサーバ侵入演習 4 コマの流れとなる．

4.　評価の枠組み

4.1　到達目標に対する自己評価

「システム管理 II」で掲げる 13 の到達目標について，各受講生はどの程度その能力を身につけているか，事前・事後で自己評価を行い，その伸びで演習の効果を測定する．

自己評価質問項目一覧を**表 2** に示す．受講生は各質問項目に対して，「1. できない，2. あまりできない，3. ある程度できる，4. できる」から最もあてはまるものを選択する．

4.2　理解度確認テスト

サーバ構築演習・サーバ侵入体験演習の知識・技能に関わる理解度確認テストを事前・事後で実施し，自己評価と合わせて学習効果を測定する．テスト問題については，エルピーアイジャパンが公開している LPIC-2 用サンプル問題 [20] のうち本演習で実施する各種サーバ構築に関わる問題や，情報処理推進機構が実施する基本情報技術者試験・情報セキュリティマネジメント試験・情報処理安全確保支援士試験（旧・情報セキュリティスペシャリスト試験）の午前問題の過去問題 [21] からサーバ侵入演習で取り扱う内容に関わる問題を抜粋してテスト問題とした．

サーバ構築分野の問題例を**図 8** に，セキュリティ分野の問題例を**図 9** に示す．

図 8 に示した問題は LPIC-2 用サンプル問題の中の一題である．BIND を用いた DNS サーバの設定に関わる問

問. ゾーンファイルの情報を変更した際に，必ず修正しなければならないレコードを選べ．（LPIC201 サンプル問題）

1. A レコード
2. CNAME レコード
3. MX レコード
4. NS レコード
5. SOA レコード

図 8　サーバ構築分野の問題例

Fig. 8　An example question about server configuration.

問. Web サーバの検査におけるポートスキャナの利用目的はどれか．（平成 26 年秋基本情報午前問題）

1. Web サーバで稼働しているサービスを列挙して，不要なサービスが稼働していないことを確認する．
2. Web サーバの利用者 ID の管理状況を運用者に確認して，情報セキュリティポリシからの逸脱がないことを調べる．
3. Web サーバへのアクセス履歴を解析して，不正利用を検出する．
4. 正規の利用者 ID でログインし，Web サーバのコンテンツを直接確認して，コンテンツの脆(ぜい)弱性を検出する．

図 9　セキュリティ分野の問題例

Fig. 9　An example question about cybersecurity.

題であり，正解は 5 番である．図 9 に示した問題は平成 26 年秋期基本情報技術者試験午前試験の中の一題である．Nmap 等のポートスキャナの利用目的を問う問題であり，正解は 1 番である．

テストは事前・事後とも全 16 問からなる．全 16 問のうち前半 8 問がサーバ構築に関わる問題，後半 8 問がサーバ侵入演習（セキュリティ分野）に関わる問題となっている．すべての問題は選択問題で，4 択問題 14 問，5 択問題 2 問からなり，全問題解答必須，1 問 1 点の 16 点満点とした．

5.　結果と考察

5.1　演習中の受講生の様子

実験用仮想環境の構築は当初予定より時間を要した．仮想環境において Kali Linux と Metasploitable2 をゲスト OS として用意し，ゲスト OS だけが所属する仮想ネットワークを構築する必要がある．しかし，その意味が理解しにくかったようで，ゲスト OS のネットワーク設定において当初は若干混乱が見られた．また，仮想ネットワークに所属する Metasploitable2 に対して脆弱性検査を行うためには，同一の仮想ネットワークに所属する攻撃役ゲスト OS である Kali Linux に脆弱性検査ソフト Nessus をインストールする必要があるが，ホスト OS である Windows にインストールしようとする受講生が数人見られた．このため，実験環境構築は 2 コマ目にも差しかかり，以降，若干の時間調整が必要となった．

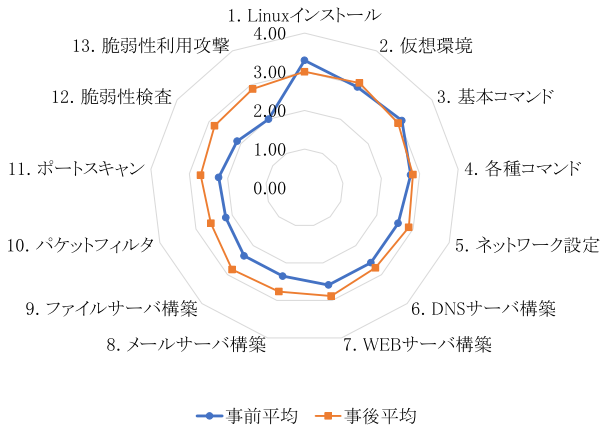

図 10　自己評価事前平均と事後平均の比較

Fig. 10　Comparison between students' pre and post self-assessment about server configuration and cybersecurity.

仮想環境における実験では，分かりやすい脆弱性をそなえた被害役マシンを対象に脆弱性検査やサーバ侵入を試みるため，受講生は想定どおりサーバ権限を奪取し，攻撃の一連の流れを理解した様子であった．一方，実験室内で自分達が構築した実機サーバを対象に攻撃を試みた場合，ただちに侵入できる脆弱性が見つかるわけではなく，侵入は成功しない．攻撃が成功しないことはセキュリティの観点からは喜ばしいことであるが，Metasploitable2 を対象に実施したのと同様に簡単に攻撃が成功すると思っていたのか，成功しないことに戸惑う受講生が見られた．

サーバ攻撃自体に興味を持ったある受講生は，自分で攻撃手法について調べるようになり，実際に稼働しているサーバに対して攻撃手法を試してみたい気持ちがあるが法令を遵守しなければならないため悩ましいと語っていた．その他の受講生からも日本の法律の厳しさを口にする声があがっていた．法令遵守教育の必要性を示すできごとであり，また，法令遵守教育が確かに効果を発揮している 1 つの証左といえる．

5.2　到達目標に対する自己評価結果

自己評価について，事前・事後の両方に回答した受講生 17 人を分析の対象とする．演習の事前と事後で平均的にどの項目が伸びているかを見るため，事前・事後の別に，質問項目ごとに平均評価値を求め，レーダチャートとして示したものが図 **10** である．評価値の計算にあたっては，できない 1 点，あまりできない 2 点，ある程度できる 3 点，できる 4 点としている．

項目 1〜4 については事前と事後は変わらないか事前が

表 3　理解度確認テスト（16 点満点）
Table 3　Summary of pre-test and post-test results (server configuration and cybersecurity, 16-point scale).

	事前	事後
平均	3.8	7.9
最低	0	4
最高	8	11
標準偏差	1.8	2.4

表 4　セキュリティ分野理解度（8 点満点）
Table 4　Summary of pre-test and post-test results (cybersecurity, 8-point scale).

	事前	事後
平均	1.3	5.3
最低	0	2
最高	3	7
標準偏差	1.1	1.6

高い結果となっている．これは本科目受講開始時点で当該内容についてすでに既習であったことによると考えられる．3 年生前期科目である「システム管理 I」において受講生は 1 人 1 台貸与された Windows ノート PC に VirtualBox を利用して仮想環境を構築し，Ubuntu および CentOS をゲスト OS としてインストールし，Linux の学習・各種コマンドの実習を行っている．また受講生は 1 人 1 台サーバ機を専用で利用しており，CentOS を各自でインストールし，こちらも Linux の学習に利用している．この経験の結果，本科目の受講時点ですでにある程度以上できていたと考えられる．

他方，サーバ構築に関する項目 5〜9 およびセキュリティに関する項目 10〜13 に関して平均点が向上していることが確認できる．1〜13 のすべての項目に関して，項目ごとに平均値の差について対応のある t 検定（5%有意水準の両側検定）を行った結果，項目 13 の脆弱性利用攻撃（事前平均 2.0，事前標準偏差 1.1，事後平均 2.9，事後標準偏差 0.8）についてのみ，t 値 $= -2.37$，P 値 $= .031$ より有意差が認められた．なお，有意ではないものの，項目 12 の脆弱性検査（事前平均 2.1，事前標準偏差 1.1，事後平均 2.8，事後標準偏差 0.8）については，t 値 $= -1.90$，P 値 $= .076$ であった．これらの結果から，サーバ侵入演習の効果が確かに表れているといえる．

5.3　理解度確認テスト結果

理解度確認テストについて事前・事後の両方を受験した受講生 16 人を分析の対象とする．事前・事後テストの結果を**表 3** に示す．

16 点満点のテストにおいて，平均点が 4.1 点上昇している．平均値の差について対応のある t 検定（5%有意水準の両側検定）を行った結果，t 値 $= -5.33$，P 値 $< .001$ より有意差が認められた．ただし，このテストはサーバ構築に関する問題 8 問，セキュリティに関する問題 8 問からなるため，ここでは授業全体として受講生の理解におよぼす効果を見ていることになる．

次に，サーバ侵入演習を通じてどの程度セキュリティに関する知識が向上したかを分析するため，理解度確認テスト 16 問のうちセキュリティに関する問題 8 問の事前事後結果を比較する．セキュリティに関する事前・事後テストの結果を**表 4** に示す．

セキュリティ分野の問題 8 問に関して，平均点が 4.0 点上昇している．平均値の差について対応のある t 検定（5%有意水準の両側検定）を行った結果，t 値 $= -7.37$，P 値 $< .001$ より有意差が認められた．サーバ侵入演習を実践した結果として，セキュリティ分野の知識が向上していることが分かった．

5.4　授業終了後の受講生のコメント

「システム管理 II」第 15 回授業終了後，17 人の受講生に授業に関して印象に残った点をあげてもらったところ，3 人がサーバ構築技術を，3 人が脆弱性利用攻撃をあげたのに対して，4 人が日本の法律の厳しさをあげた．それ以外は，4 人がコメントなし，3 人がそのほかのコメントとなっている．

脆弱性利用攻撃をあげた受講生のうち 1 人は，別途コメントとして，実際に攻撃を実践したいが罪を犯したくないのでできない，と述べた．なお，印象に残った点として 4 人が言及した日本の法律とは，脆弱性利用攻撃を実行しようとする際に関わる法律を指している．

先述のとおり，本演習の受講生は中国からの留学生であり，日本の法律について学ぶ機会や学んだ経験はきわめて少ない．それゆえに，本演習の中で，サイバー攻撃に関連する日本の法律について自分で調べ，自分でまとめ，その内容をふまえて誓約書に署名・提出したことが，印象に残る結果につながっていると考えられる．このように，法令遵守について学ぶ機会が学んだ攻撃技術の悪用を防ぐ抑止力となりうることが示唆される結果となっている．

5.5　サーバ侵入演習教育カリキュラムの効果と課題

サーバ侵入演習は，脆弱性を利用したサーバ侵入等の攻撃体験を通じて，実際の攻撃手法や攻撃者の行動を知り，セキュリティ分野の知識習得の契機とする目的で実施した．カリキュラムを工夫し，演習内容を検討することで，専門情報教育の一環として大学学部であっても攻撃体験演習の実施が可能であること，事前事後の自己評価および理解度確認テストからは，本演習が受講生のセキュリティ分野に関する知識を向上させることが確認できた．また授業中や授業後の受講生のコメントから，法令遵守について学

ぶ機会が学んだ技術を悪用させない抑止力となりうることが確認できた．攻撃手法を授業において扱ううえでは，時機を逸せず，必ず法令遵守について学ぶ機会を設けるべきであると考える．

本演習カリキュラムの継続性についてであるが，サーバ侵入演習において取り扱った攻撃は，仕込まれたバックドアを利用して侵入するという簡単で実行しやすい事例である．典型的で被害が深刻になりうる攻撃を取り上げる方が分かりやすいと考えてのことであるが，時代とともに現れる脆弱性とそれを狙う攻撃のバリエーションは多岐にわたる．そのため事例については時代に応じたものを取り上げる必要が生じる可能性がある．

しかし，仮想環境や実機サーバ等の実験環境構築に関わる知識・技術は一般的なものであり，将来にわたって利用可能である．サーバ侵入攻撃において用いた Nmap や Nessus，Netcat，Metasploit Framework 等も広く認め知られているツールであり，攻撃対象の探索，脆弱性調査，脆弱性利用攻撃の手順もオーソドックスなものを示している．法令遵守教育の重要性も薄れることはないと考える．そのため，本演習の内容・構成，カリキュラムの枠組みは相応の継続性を有すると期待される．

なお，本研究では，関連科目の内容や配置も含めてカリキュラムを検討しており，サーバ侵入演習の実施に先立って，ネットワークやサーバ構築について学んでいるため，その知識・技術を前提とした本演習の実践が可能となった．サーバ侵入演習を一般情報教育の一環として実施する場合等は，環境構築やネットワーク設定で躓くことが考えられ，別途カリキュラムの検討が必要と考える．

残された課題についてであるが，「システム管理 II」では，サーバ構築とサーバ攻撃体験を重視しており，防御については第 10 回授業において，TCP Wrapper と iptables について学ぶにとどまっているため，防御面の学習が十分とはいえない．ただし，後に続く 4 年生前期科目「情報セキュリティ論」において防御面の学習を実施することになっているため，サーバ侵入演習は「情報セキュリティ論」への動機づけの役割を持たせている．本稿で提案したカリキュラムとは異なり，情報セキュリティを扱う独立した科目でサーバ侵入演習のような攻撃実践演習を実施する場合は，攻撃演習の後の防御面の学習を手厚くする必要があるだろう．

また，本攻撃実践演習により，関連するセキュリティ分野の知識向上が確認できたが，実社会でサイバー攻撃によって現実にどのような被害がもたらされているか学習することが重要であると考える．グループでケーススタディを行う等，サイバー攻撃がもたらす社会的影響について学ぶ機会を設けることが，セキュリティ分野に対する学習意欲向上に有効である可能性がある．

なお，本研究では，演習の事前事後で自己評価と理解度確認テストを行い，自己評価数値およびテスト得点の統計的有意な向上が見られたため，本演習が教育効果を有するとした．しかし，授業の構成上，統制群を置くことができていないため，本演習以外の要因による成績向上の可能性は厳密には排除できていない．ただし，サーバ構築演習やサーバ侵入演習はもっぱら本授業においてのみ行っているため，これに関わる知識・技術の向上は本授業に起因するものと推測している．

6. おわりに

本研究では，脆弱性を利用したサーバ侵入演習を大学学部の専門情報教育の一環として実施可能な形で提案・実践し，その教育効果を明らかにすることを目指した．サーバ侵入演習は，サイバー攻撃の攻撃者の行動を知る機会を受講生に提供し，セキュリティ分野の知識習得の契機を与える目的で導入した．演習では，各自が管理するノート PC の上に VirtualBox を利用して仮想環境を作り，攻撃役仮想マシンとして Kali Linux を，被害役仮想マシンとして Metasploitable2 を設け，Nmap，Nessus，Netcat，Metasploit Framework を利用してサーバ攻撃実験を行った．また，受講生各自が実験室内に構築したサーバへの攻撃実験とサイバー犯罪関連法規の学習も行った．カリキュラムを工夫し，演習内容を検討することで，専門情報教育の一環として大学学部であっても攻撃体験演習の実施が可能であること，事前事後の自己評価および理解度確認テストからは，本演習が受講生のセキュリティ分野に関する知識を向上させることが確認できた．また受講生のコメントから，法令遵守について学ぶ機会が学んだ技術を悪用させない抑止力となりうることが示唆された．

参考文献

[1] 八木　毅，秋山満昭，森　達哉，針生剛男，後藤滋樹：産学連携によるサイバーセキュリティ教育分野の確立，信学技報，Vol.115, No.80, pp.3–8 (2015).

[2] 後藤厚宏，曽根秀昭，宮地充子，藤川和利，砂原秀樹：実践セキュリティ人材育成コース SecCap，コンピュータソフトウェア，Vol.34, No.1, pp.1_18–1_23 (2017).

[3] Harris, J.: Maintaining ethical standards for a computer security curriculum, *Proc. 1st Annual Conference on Information Security Curriculum Development*, pp.46–48 (2004).

[4] 鈴木大助：セキュリティ意識の向上を目的としたサーバ侵入演習の導入計画，電子情報通信学会技術研究報告，Vol.117, No.286, pp.103–106 (2017).

[5] 鈴木大助：セキュリティ意識の向上を目的としたサーバ侵入演習の実践と評価，電子情報通信学会技術研究報告，Vol.IEICE-118, No.152（SITE), pp.131–136 (2018).

[6] Yang, J., Wang, Y. and Reddington, Y.: Integrate Hacking Technique into Information Assurance Education, *2016 30th International Conference on Advanced Information Networking and Applications Workshops* (*WAINA*), Crans-Montana, Switzerland, pp.381–387 (2016).

[7] Mateti, P.: A laboratory-based course on internet security, ACM SIGCSE Bulletin, Vol.35, No.1, pp.252–256 (2003).
[8] Trabelsi, Z. and Ibrahim, W.: A hands-on approach for teaching denial of service attacks: A case study, *Journal of Information Technology Education: Innovations in Practice*, Vol.12, pp.299–319 (2013).
[9] 立岩佑一郎，岩崎智弘，安田孝美：仮想マシンネットワークによる継続的なクラッキング防衛演習システム，電子情報通信学会論文誌 D，Vol.96, No.7, pp.1585–1594 (2013).
[10] 福山和生，谷口義明，井口信和：仮想マシンを活用したネットワークセキュリティ学習支援システムの実装と評価，情報処理学会論文誌，Vol.57, No.3, pp.931–935 (2016).
[11] Oracle VM VirtualBox, available from ⟨http://www.oracle.com/technetwork/jp/server-storage/virtualbox/overview/index.html⟩ (accessed 2017-10-19).
[12] Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution, available from ⟨https://www.kali.org/⟩ (accessed 2017-10-19).
[13] Metasploitable 2 Exploitability Guide, available from ⟨https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guide⟩ (accessed 2017-10-19).
[14] Nessus Home, available from ⟨https://www.tenable.com/products/nessus-home⟩ (accessed 2017-10-19).
[15] Nmap: the Network Mapper - Free Security Scanner, available from ⟨https://nmap.org/⟩ (accessed 2018-08-03).
[16] The GNU Netcat – Official homepage, available from ⟨http://netcat.sourceforge.net/⟩ (accessed 2018-08-4).
[17] metasploit, available from ⟨https://www.metasploit.com/⟩ (accessed 2017-10-19).
[18] 鈴木大助：ジグソー学習法を取り入れた新入生を対象とするネットワーク利用ガイダンスの実践と評価，情報処理学会論文誌 教育とコンピュータ，Vol.4, No.2, pp.14–22 (2018).
[19] 情報セキュリティ関連の法律・ガイドライン，入手先 ⟨http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/legal/index.html⟩（参照 2018-06-24）.
[20] サンプル問題・例題解説 | Linux 技術者認定試験，入手先 ⟨http://www.lpi.or.jp/ex/⟩（参照 2017-10-15）.
[21] 情報処理技術者試験・情報処理安全確保支援士試験過去問題，入手先 ⟨https://www.jitec.ipa.go.jp/1_04hanni_sukiru/_index_mondai.html⟩（参照 2017-10-15）.

鈴木 大助　（正会員）

1999 年京都大学理学部理学科卒業．2001 年京都大学大学院情報学研究科修士課程修了．2004 年京都大学大学院情報学研究科博士課程修了．博士（情報学）．東京理科大学工学部経営工学科助手，東京工科大学コンピュータサイエンス学部助教，北陸大学情報センター講師，未来創造学部講師，経済経営学部講師を経て，2018 年より同准教授．情報教育，教育工学の研究に従事．CIEC 会員．