G-47

サイバーセキュリティにおける 教育効果の高い学習方法についての考察

西山 友梨†　　川橋 裕‡
Nishiyama Yuri　Yutaka Kawahashi

1. はじめに

近年，スマートフォンなどの情報機器の普及により，誰でも簡単に Web サイトへアクセスでき，ショッピングや銀行取引などのオンラインサービスが広く利用されるようになった．一方で，利便性の向上とともにサイバー攻撃も増加・高度化しており，それに対抗する人材の不足が社会的な課題となっている．こうした背景から，サイバーセキュリティ教育の重要性が高まっている．

現在の教育では，セキュリティインシデントへの対応力を養う「防御者視点」の学習が中心である．しかし，攻撃の手法や思考を理解する「攻撃者視点」の教育は限られており，その学習効果の検証も十分ではない．また，座学と演習の順序が学習成果にどう影響するかも明らかになっていない．

本研究では，防御者視点と攻撃者視点の教育効果に加え，演習と座学の順序が学習成果に与える影響を比較・分析することで，より効果的なサイバーセキュリティ教育手法の確立を目指す．

2. 関連研究・既存の学習方法

2.1 関連研究

情報セキュリティ教育のための標的型攻撃実演システムの構築[1]では，情報セキュリティを学び始めた初学者を対象に，攻撃者視点から学ぶことを目的とした標的型攻撃実演システムを提案している．従来のセキュリティ演習は，防御中心で一定の IT スキルを前提としているため，知識を深めにくいという課題があった．システムとしては，架空企業を標的に，偵察・配送・遠隔操作・目的実行といった一連の攻撃を体験させ，攻撃の流れを実感できる構成となっている．演習後には座学を行い，記憶の定着を図っている．結果として，攻撃の仕組みへの理解やセキュリティ意識，学習意欲の向上が確認された．一方で，専門用語の理解が難しいという課題があり，今後は初学者向けに用語解説や事例の追加など，演習内容の調整が求められている．

2.2 既存の学習方法

インシデントレスポンス演習とは，和歌山大学で BasicSecCap[2]の演習科目として開講されている，PBL形式の演習である．この演習は4日間の集中講義として開講され，受講生はチームを組み，マネジメントや作業員，顧客対応などの役割を分担しながら，さまざまなインシデント対応に取り組む．演習では，スパムメールをきっかけとしたアカウント乗っ取りや，偽DHCPサーバによる不正誘導など，複数の事例を通じて，インシデントの切り分けや適切なレスポンス手法を実践的に学習する．また，ロールプレイを取り入れることで，ユーザとの情報のやり取りやチーム内での情報共有といったコミュニケーションの重要性も体験的に理解できるよう設計されている．このように，本演習は技術的スキルの向上だけでなく，協働力や応用力の育成にも重点を置いた，実践的かつ総合的な教育プログラムとなっている．

3. 提案手法

本研究では，防御者視点と攻撃者視点の学習効果を比較するため，双方の視点 に基づいた座学及び演習を設計した．これにより，サイバーセキュリティ教育における学習順序の違いや防御者視点と攻撃者視点の教育が学習効果にどのような影響を与えるか検証する．

3.1 前提条件

教育にあたっての前提条件を以下に示す．この前提条件を基に実験を行った．

(1) 防御の重要性を中心に据えること．攻撃手法を紹介する際は必ず対応する防御策も併せて提示し，防御の重要性を理解させる．たとえば，ポートスキャンにはその検出や遮断方法を説明する．

(2) 実際の攻撃行為を排除すること．実際の攻撃ツールやコードの使用は避け，攻撃の意図や影響を概念的に学習させる．

(3) 学習管理の強化をすること．攻撃者視点の演習は，講義内かつ責任者の監督下でのみ実施し，不適切な利用を防ぐ体制を整える．

3.2 防御者視点の学習内容

防御者視点の教育は，座学と演習の 2 つの手法によって構成されている．まず座学では，サイバー攻撃の種類やその概要，各攻撃に対する有効な対策方法について体系的に学習する．対象とする攻撃は，外部から内部を狙うものに限定し，具体的には「DoS 攻撃」「DDoS 攻撃」「SQL インジェクション」「クロスサイトスクリプティング」「パスワードリスト攻撃」「ディレクトリトラバーサル」の 6 種を扱う．それぞれの攻撃に対して，ファイアウォールや IDS/IPS の導入，IP 制限などの基本的な防御策を紹介し，対策の考え方を理解することを目指す．

一方，演習では和歌山大学で開講されているインシデントレスポンス演習を活用する．参加者は，サイバー攻撃によって発生したインシデントに対応するシナリオに沿って，被害状況の分析や侵入経路の特定，封鎖，被害範囲の最小化などの実践的タスクに取り組む．演習を通して，技術的スキルだけでなく，状況判断やチーム内での情報共有といった対応能力も養うことができる．このように，座学と演習を組み合わせることで，理論と実践の両面から防御力を高める教育を実現している．

3.3 攻撃者視点の学習内容

攻撃者視点の教育方法は，防御者視点と同じく座学と演習の二種類を用意する．サイバー攻撃の全体像を体系的に理解させることを目的とし，その基盤としてサイバーキルチェーンのモデルを採用する．まず座学は，各フェーズに

†和歌山大学大学院 システム工学研究科 川橋研究室
‡ 和歌山大学学術情報センター

おける具体的な手法や考え方を学び，攻撃の流れを包括的に把握する構成とする．具体的には，偵察段階であれば，隠密偵察と威力偵察で攻撃者が用いる情報収集の方法について説明する．例えば，ターゲットとなる企業のホームページからメー ルアドレスなどの情報を取得できることや，ポートスキャンなどを説明する．その後，偵察段階で有効な対策となる，ホームページには安易に情報を載せないといった対策を紹介する．そのフェーズで実施できる有効な対策方法について説明することで，サイバーキルチェーンの各段階に対する理解を深める．

演習は，関連研究で紹介した標的型攻撃実演システムを活用する．これにより，サイバーキルチェーンの流れに沿って参加者に実際に攻撃してもらうことで，サイバー攻撃への理解を深める．

4. 実験

4.1 実験概要

本実験は，インシデントレスポンス演習にて実施した．ここでは参加者を二つのグループ A と B に分けた．それぞれチーム内の人数は偏りが出ないようにしている．グループについての詳細を以下の表 1 に示す．

表 1 ：グループ

グループ	所属学部の主な区分	人数	授業形式
A	ネットワーク情報学メジャー	34 人	オンライン (ライブ形式)
B	知能情報学メジャー	34 人	対面授業

所属学部の主な区分として，ネットワーク情報学メジャーと知能情報学メジャーがあるが，こちらはいずれも情報系のメジャーである．授業形式に関して，グループ A はオンライン(ライブ形式)，グループ B は対面授業となっているのは，台風による警報の発令により対面実施が不可能となったためである．

そして，提案手法で述べた防御者視点と攻撃者視点の学習内容を基に 4 つのカリキュラムを用意した．カリキュラムについての詳細を以下の表 2 に示す．

表 2 : カリキュラム

カリキュラム	学習内容	所要時間
1	防御者視点の演習	60 分
2	防御者視点の座学	60 分
3	攻撃者視点の演習	60 分
4	攻撃者視点の座学	60 分

インシデントレスポンス演習では，表 2 で示した 1〜4 のカリキュラムを基にグループ A と B に講義を行った．講義の流れとしては，グループ A と B でカリキュラムの実施順序を変えている．講義順序について以下の表 3 に示す．

表 3 : 講義の流れ

グループ	カリキュラムの順序
A	1→2→3→4
B	2→1→4→3

講義内容に関してはグループ A と B の両方同一のものとなっている．

4.2 評価概要

評価は 3 つの指標で構成している．

1. テストの点数
   本実験ではグループ A と B の両方にテストを実施することで学習効果を算出する．具体的なテスト実施の詳細について以下の図 1 に示す．

	I	II	III	IV	V
A	1 → 2 → 3 → 4				
B	2 → 1 → 4 → 3				

図 1 : テスト実施の流れ

   A グループ と B のインシデントレスポンス演習開始前のテストを I とし，事前に参加者の学習状況を把握する．その後 A と B の一つ目のカリキュラム終了後のテストを II，その次のカリキュラム終了後のテストを III，IV，V とし実施す る．このように，カリキュラムが一つ終了するごとにテストを実施すること により，一つ一つのカリキュラムの学習効果を計る．テスト内容については 100 点満点とし，29 点分が防御者視点の内容，29 点分 が攻撃者視点の内容，42 点分が防御者視点と攻撃者視点の両方の視点が必要となる内容としている．
2. 参加者の回答の変化
   テストの点数ではわからない参加者の思考の変化や柔軟性を測る．
3. 講義評価アンケート

5. 実験結果

5.1 テストの点数

本実験で実施したテストの平均点を以下の図 2 に示す．

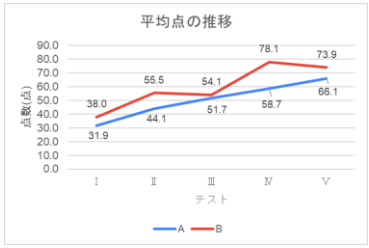
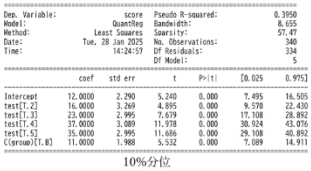


図 2 : 平均点の推移

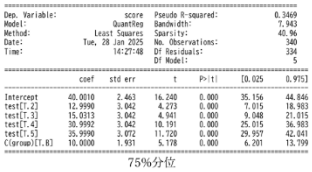
演習を先に行ったグループ A は，テストの得点が段階的に安定して伸びていく傾向が見られた．一方，座学を先に行ったグループ B は，座学後に得点が上昇するものの，その後やや低下する傾向が見られた．学習内容別に見ると，防御者視点の学習は演習を先に行った方が効果的であり，攻撃者視点では座学を先に行った方が理解が深まりやすいという傾向が読み取れる．全体としては，演習と座学の順序による最終的な学習効果に変わりはないことがわかった．

分位点回帰分析の結果を以下の表 4 に示す．

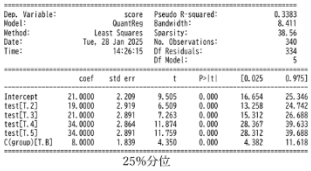
表 4 : 分位点回帰分析の結果



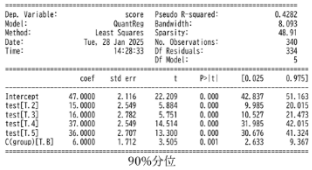
10%分位



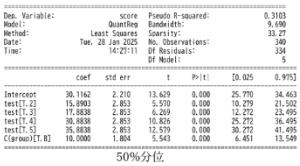
75%分位



25%分位



90%分位



50%分位

結果より，テストがI〜Vに進むにつれてテストの点数に対する影響が増大し，特に IV と V で顕著になることがわかる．そして，全体的にグループ B の点数が高いことから，グループ B の方が点数の伸びが大きいといえる．

共分散分析の結果を以下の表 5 に示す．

表 5：共分散分析の結果

Dep. Variable:	score	R-squared:	0.130
Model:	OLS	Adj. R-squared:	0.124
Method:	Least Squares	F-statistic:	20.12
Date:	Tue, 28 Jan 2025	Prob (F-statistic):	7.18e-09
Time:	15:04:52	Log-Likelihood:	-1113.6
No. Observations:	272	AIC:	2233.
Df Residuals:	269	BIC:	2244.
Df Model:	2		
Covariance Type:	nonrobust		

	coef	std err	t	P>|t|	[0.025	0.975]
Intercept	49.5940	2.517	19.700	0.000	44.638	54.550
C(group)[T.B]	9.2481	1.819	5.085	0.000	5.667	12.829
covariate	0.1730	0.069	2.526	0.012	0.038	0.308

Omnibus:	0.158	Durbin-Watson:	1.630
Prob(Omnibus):	0.924	Jarque-Bera (JB):	0.046
Skew:	-0.022	Prob(JB):	0.977
Kurtosis:	3.046	Cond. No.	107.

結果より，初回の成績が良い人ほど，その後の成績も高くなる傾向があることを示しているが，その影響は比較的小さいことがわかる．

各問題の正答率の変化を比較した結果，演習を先に行ったグループ A では，全体的にほとんどの問題で正答率が向上し，防御者視点・攻撃者視点の両方でバランスよく学習効果が見られた．一方，座学を先に行ったグループ B では，防御に関する一部の問題で正答率が下がる傾向が見られたものの，全体的には一定の向上が確認された．特に，どちらのグループでも，攻撃者視点の学習を終えた後は，攻撃と防御の両方の理解が求められる問題において大きく正答率が上がっており，攻撃の仕組みを深く理解することが防御にも効果的であることが示唆された．

5.2 参加者の回答の変化

演習を先に行ったグループ A では，学習が進むにつれて回答がより具体的・実践的になっていく傾向があった．攻撃手法を挙げる設問では，回答に多様性が見られ，複数の攻撃手法を挙げる者が増加した．防御策に関する設問においても，ファイアウォールの導入といった基本的な対応に加え，特定の IP アドレスからの通信遮断，ポートの制限，IDS/IPS の活用など，現実的かつ多様な対応策が回答されるようになった．さらに，フィッシング対策などに関しても，URL の確認にとどまらず，ブックマークの利用や証明書の確認といった，より実践的な内容が増加していた．

一方，座学を先に行ったグループ B では，回答内容が模範的な形式に収まる傾向が強く，定型的な回答が多く見られた．座学で学んだ内容に沿った正答が多く，基礎的な理解は定着しているものの，応用的な発想や発展的な対策までには至らないケースが目立った．また，テストを重ねても，設問ごとの回答の変化が少ないものも多く，演習によって得られる気づきや視野の広がりが十分に生まれていなかったことがうかがえる．

以上より，演習を先に行うことで，受講者はより実践的かつ多面的な視点を獲得しやすくなる一方で，座学を先に行った場合は，知識の定着には有効であるが，応用力や柔軟な対応力の習得には限界があることが示唆される．

5.3 講義評価アンケート

講義評価アンケートの結果から，防御者視点の演習は他と比べてやや難易度が高い一方で，学習内容のバランスや難易度設定は概ね適切であると評価されている．特に，約7〜8 割の参加者が座学より演習の方が理解に効果的と感じており，その理由として「実体験による理解のしやすさ」や「座学だけでは具体的なイメージが持ちにくい」といった意見が挙げられた．

また，学習の順序に関しては，演習を先に行ったグループ A では「復習としての座学が有効」，「座学を先に実施したほうが演習で理解しや すい」といった意見が寄せられ，座学を先に行ったグループ B では「座学で理解したうえで実践するのが効果的」との意見が見られた．さらに，実習を通じて「実際の対応力やコミュニケーションの重要性」，「攻撃者視点の有用性」への気づきがあったとの声も多く，実践的な学びの有効性が示された．一方で，オンライン形式で実施されたグループ A からはツールの使いにくさや対面との比較での不満も見られた．

6. 考察

6.1 座学と演習の効果

座学と演習の効果として，テストの点数の向上という観点では，座学を先に行い，その後に演習を行う方が効果的であると考えられる．しかし，サイバーセキュリティ人材の育成という観点では，幅広く具体的な対策を考えられる力が重要であり，その点で演習から座学の学習順序の方がより効果的であると考えられる．

6.2 防御者視点と攻撃者視点の効果

テストの点数の向上という点では，攻撃者視点の学習の方が効果は大きく，特に攻撃と防御の両面を問う問題で正答率が大きく上がった．これは攻撃の理解が防御力の向上につながったことを示している．

また，攻撃者視点の学習後には回答の具体性が増し，実践的な思考力の育成にも効果が見られた．一方で，防御者視点も多くの参加者が有用だと評価しており，どちらの視点も重要であるといえる．

6.3 授業形式の効果

オンライン(ライブ形式)よりも，対面授業の方が効果は高いと考える．講義評価アンケートでも，「Discord が少し使いにくかった」，「オンライン形式はメリットではあるが，本演習では好ましくないと感じた」といった意見が多数寄せられた ためだ．

6.4 学習視点と手法に関する統合的考察

サイバーセキュリティ人材の育成においては，「演習→座学」の順序で学習を実施し，攻撃者視点と防御者視点をバランスよく取り入れ，対面授業を活用することが，教育効果の高い学習方法である．これにより，実践的なスキルを身につけつつ，体系的な知識を整理し，より効果的な防御策を立案できる能力を養うことができる．

7. 今後の課題

本研究では，授業形式について，オンライン(ライブ形式)よりも，対面授業の方が効果は高かった．しかし，台風による警報の発令により対面実施が不可能となるような

不測の事態は，今後も起こることが考えられる．そのため，オンライ ン(ライブ形式)においても，教育効果の高い学習方法を確立する必要がある．そして，今回は防御者視点を先に実施した後に攻撃者視点を実施したため，次回は攻撃者視点を実施した後に防御者視点を実施することで，攻撃者視点と防御者視点のどちらの方が効果が高いかをより明確にすることができると考える．

参考文献

[1] 佐尾山裕司：情報セキュリティ教育のための標的型攻撃実演システムの構築
和歌山大学修士論文，2024
[2]和歌山大学：和歌山大学 BasicSecCap
https://www.wakayama-u.ac.jp/dtier/seccap/
(参照 2025-07-24)