G-26

セキュリティ学習用シミュレーション演習システムの開発

年見 卓瞭†　　川橋 裕‡
Takaaki Toshimi　Yutaka Kawahashi

1. はじめに

近年,サイバー攻撃の増加とセキュリティ人材の不足が深刻な問題となっている.「NICTER 観測レポート 2023」によると,2023 年では 1IP アドレスあたりで約 226 万パケットが観測され,この記録は観測開始以降最も多い値である[1].加えて,サイバー攻撃の件数は年々増加し,攻撃手法も高度化・複雑化している.例えば,ランサムウェア攻撃においては,従来は不特定多数を対象とし,攻撃をして引っかかった端末のみにデータの暗号化などを行っていた.しかし,新たな攻撃方法では,攻撃対象が引っかかった端末だけでなく,同一ネットワーク上のファイルサーバのデータも暗号化・窃盗を行う「二重恐喝」型の攻撃に進化している[2]. 上記のような脅威に対抗するためには,高度な専門知識を持つセキュリティ人材 が不可欠である.しかし,NRI セキュアテクノロジーズが日本の企業に対して行った調査によると,約 9 割の企業でセキュリティ人材が不足していると回答している [3]. この人材不足の主な原因は,デジタル技術の急速な普及に伴い,セキュリティ対策に求められる技術や知識の幅が広がったことにある.従来のセキュリティの範囲は主に「オフィス内」と限定的であったが,現在では IT によって支社や工場などの各拠点とも連携している.したがって,守るべき場所が増え,必要数も増加している[4]. 情報セキュリティ分野では依然として人材不足が続いているため,企業や組織を脅威にさらすリスクを高めている.加えて,従業員のセキュリティ意識の不足, セキュリティ教育を実施する専門人材の不足なども問題として挙げられる.

本研究では,このような状況を踏まえ,セキュリティ意識向上とセキュリティ教育のサポートを目的としたシミュレーションを作成する.本シミュレーションでは,事前に用意したネットワーク構成図に対して SQL インジェクションや標的型メールなどの疑似的な攻撃をシミュレートし,それに対する防御方法を学ぶことができる.本シミュレーションを通じて,利用者は実際に攻撃や防御の戦略を学びながら,セキュリティの基本的な概念やリスク管理を理解し,実践的なセキュリティスキルを向上させることができる.

2. 関連研究

「脆弱性対策教育のための e ラーニングシステムの開発と評価」では,VulCES(Vulnerability Countermeasures E-learning System)と呼ばれる脆弱性対策教育システムの開発とその効果検証が行われている［5］.本システムは,特にクロスサイト・スクリプティング攻撃の手法とその対策について学習することを目的としており,利用者が攻撃の概要,具体的な手法,対策を効果的に習得できるよう,シナリオ型の教育手法が採用されている.また,コンテンツの一部には 3D アニメーションが取り入れられており,利用者の学習意欲の維持や e ラーニング特有の単調さを軽減する工夫がなされている.さらに,意図的に脆弱性を含んだウェブアプリケーション「WebGoat」を教材として活用することで,受講者は実際にクロスサイト・スクリプティング攻撃を模擬体験しながら,攻撃の仕組みや防御手法への理解を深めることができるよう設計されている.一方で,いくつかの課題も挙げられる.まず,WebGoat の使用により,利用者が攻撃手法を深く理解することができる反面,実際の攻撃行為に悪用されるリスクが存在するという懸念が挙げられている.また,学習コンテンツに含まれる動画のテンポが速すぎることや,表示される文章が長文かつ複雑であることから,全ての内容を十分に理解・吸収するのが困難であるという点も課題として報告されている.

和歌山大学院　システム工学研究科　知能科学クラスタ
和歌山大学 学術情報センター

3. 提案システム

3.1　システム概要

本シミュレーションは,レッドチーム(攻撃側)とブルーチーム(防御側)の役割を実際に体験することで,ネットワークセキュリティに対する理解とセキュリティリテラシーを高めることを目的としている.実施人数は一人または二人を想定している,シミュレーション上にはネットワーク図と共に,サイバー攻撃やその防御方法が表示され,利用者はそれを基に攻撃や防御を選択して実行する.一人で行う場合,攻撃と防御を交互に行い,攻撃方法や防御方法を選択することで,さまざまな事象を検証し,実際のセキュリティ対応を学ぶことができる.二人で行う場合は,攻撃役と防御役に別れ,攻撃役が攻撃を実行し,防御役がその攻撃に対して防御を行う形で 進行する.これにより,攻撃者と防御者の両方の視点からセキュリティ対策を深く理解することができる.さらに,初心者でも安心して取り組めるように,シミュレーションの概要や使い方を解説するチュートリアルも用意している.これにより,ユーザーは操作方法を学びながら,実践的なサイバーセキュリティ対応のスキルを向上させることができる.総じて,本シミュレーションは,攻撃と防御の役割を交互に体験することで,実際のサイバー攻撃に対する理解を深め,セキュリティリテラシーを向上させることにつながる.

3.2 システム構成

本節では，提案システムのシステム構成について述べる.全体のシステム構成図を図 1 に示す.

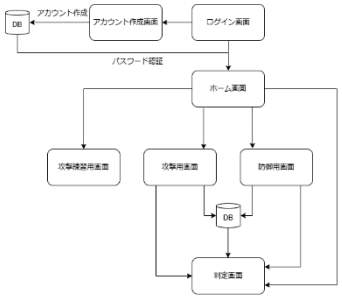

図 1　システム構成図

まず,図 1 に示されたログイン画面にアクセスする.利用者は,ユーザーネームと パスワードを入力することで,ホーム画面に遷移する.ホーム画面からは,「初めに」「攻撃用画面」「防衛用画面」「判定画面」に遷移することができる.

3. 2. 1 初めに

「初めに」の画面では,「ブルートフォース攻撃」「SQL インジェクション攻撃」「標的型メール攻撃」の 3 種類の攻撃練習を提供している.それぞれの攻撃について,攻撃の概要と,それによって引き起こされる可能性のある被害についての説明をする.同時に本シミュレーションの使用方法についても解説を行う.

3. 2. 1 攻撃用画面・防御用画面

本シミュレーションにおける「攻撃用画面」を図 2 に示す.攻撃画面および防御画面で行う操作はほとんど同じであるため,ここでは攻撃画面を例に説明を行う.攻撃画面では,ネットワーク図を用いて攻撃を実行する.まず,図 2 の右下に表示されている攻撃方法を選択する.攻撃方法を選択すると図 2 の右側に攻撃方法の概要と攻撃元,攻撃対象を選択するオプションが表示されそれぞれを選択した後,決定ボタンを押すことで攻撃を実行できる.ネットワーク図において,攻撃が実行された場所の背景を赤くすることで,後からでもどこに実行したかわかりやすくしている.始めは攻撃手段が限られているが,不正アクセスやネットワーク侵入などの攻撃を実行することで新たな攻撃方法が追加される.これは,サイバー攻撃の手順を再現している.攻撃および防御はそれぞれ最大 5 回まで実行することが可能である.攻撃または防御を終了する場合,図 2 の左下にある登録ボタンを押すことで,図 2 の上部に表示されている ID と紐づいてデータベースに登録することができ,判定の時に用いられる.

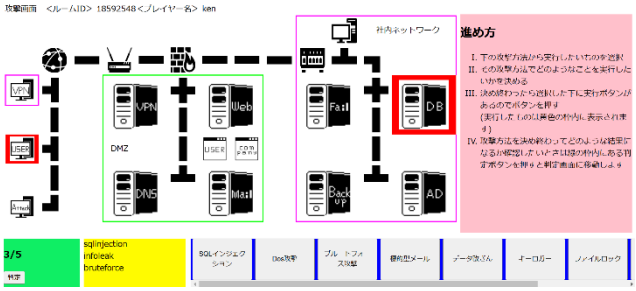

図 2　攻撃用画

3. 2. 1 判定画面

判定画面では,画面上部には,攻撃 ID および防御 ID を入力するボックスが設置されている.判定を行いたい攻撃と防御の各 ID を入力することで,データベースに登録されている攻撃方法・防御方法が判定画面に反映される.反映された攻撃方法および防御方法は画面下部の赤と青で囲われた部分に表示される.加えてネットワーク図の防御方法が設定された場所が青くなる. 判定の方法は,攻撃の 1 つ目から順番に選択された防御方法に対して攻撃が通るかどうかを確かめることで判定を行う.攻撃が通ることでレッドチームに点数が加算され、攻撃を防ぐことでブルーチームに点数が加算される。最終的に獲得した点数で勝敗を決める.

4. 実験

4. 1 実験概要

本研究では,開発したシミュレーションを被験者に実際に体験してもらい,その後アンケート調査を実施することで,シミュレーションの有効性や操作性,理解度への影響を評価する実験を行った.被験者は合計 8 名で構成され,内訳は修士課程 1 年の学生が 2 名,学部 4 年の学生が 3 名,学部 3 年の学生が 3 名である.なお,修士 1 年および学部 4 年の被験者については,所属研究室で実施・運用している「危機管理コンテスト[6]」や「インシデントレスポンス演習[7]」に従事した経験があり、情報セキュリティに関する一定の知識や実践的なスキルを有していると判断される。一方で、学部 3 年の被験者については、前述のコンテストや演習への参加経験がなく、情報セキュリティに関する体系的な学習も行っていないことから、本実験においては「初学者」として位置づける。このように、セキュリティ知識の有無に応じて被験者を分類することで、本シミュレーションが異なる知識レベルの利用者に対してどのような影響を与えるかについても分析可能となる。

4. 2 演習内容

演習では,いくつかのフェーズに分かれて構成されている。まず初めに,参加者がシミュレーションの基本的な操作方法および各種攻撃手法の概要を理解できるよう,「導入フェーズ」を実施した.この導入により,参加者はシミュレーション全体の流れや,実装されている攻撃手法の概要を把握することが可能となる.

次に「攻撃フェーズ」において,参加者は複数の攻撃手法から選択し攻撃を実行し,その後判定を行う.その結果では,各攻撃の影響や対策方法が提示されるため次の防御フェーズにおいてこれらの情報を参考にすることができる.

続く「防御フェーズ」では,攻撃フェーズの判定を参考にし,攻撃を防ぐための防御方法を防御手法から選択・実行する.再び判定に移り,攻撃が防御できることを確認する.

さらに,防御を突破するために新たな攻撃処方を参加者が考案し実行する.このように攻撃と防御を交互に繰り返し実行することにより,参加者は攻撃者と防御者のそれぞれの視点からサイバーセキュリティの知識を実践的に学ぶことができる.

最後に, 本シミュレーションがセキュリティ教育に有用性があるかを確認するために,参加者に対してアンケートを実施した.

5. 実験結果

本システムの有用性および操作性を評価するために,5 段階評価形式による 6 問の選択式設問と,自由記述による「よかった点」「改善点」「追加してほしい点」の項目を含むアンケート調査を実施した.全体として,すべての項目において高評価が得られた.特に「攻撃の概要が初心者にも理解しやすかったか」や「シミュレーションの使い方に関する説明が十分であったか」といった設問では,全ての参加者が肯定的に評価しており,導入部分の分かりやすさが高く評価された.また,「攻撃者の視点の理解」や「セキュリティに対する理解の深化」に関する設問でも,参加者全員が学びにつながったと回答しており,実践的な内容が学習効果を高めたことが示唆される.

一方で,「フィードバックの有用性」に関しては一部に中立的な評価も見られ,改善の余地があることが示された.また,自由記述では,「攻撃によってどのような情報が取得されたかが分かりにくい」「攻撃手法や防御方法の説明が不十分」といった意見があった.

一方で肯定的な意見としては,「攻撃と防御の両方を簡単に学べる点」「専門用語の説明が丁寧であった点」「アタックサーフェイスの広さを理解できた点」などが挙げられ,特に初学者にとって有効な教材として機能していることが確認された.以上の結果から,本システムはセキュリティ教育において有効な教材となり得ることが示されるとともに,今後はフィードバックの充実やコンテンツの拡充を通じて,より高い教育効果を目指す必要があると考えられる.

6. 考察・今後の課題

6.1 考察

まず,関連研究と比較した評価を行う. 脆弱性対策教育のための e ラーニングシステムの開発と評価という論文に基づくシステムとの比較を行う.論文内で指摘された改善点として,学習内容のムービーが速すぎてすべてを吸収できない,または文章が長すぎて理解が追いつかないという点が挙げられている.しかし,本シミュレーションにおいては,ユーザーが自分のペースで学習を進め,必要に応じて迅速に復習を行うことができるため,上記のような問題が発生しにくいという利点がある.次に,アンケートの結果から本シミュレーションの有用性を考察する.本研究では,セキュリティ学習用のシミュレーションを開発した.アンケートの結果から,初心者でも使いやすく,セキュリティに関する知識やセキュリティリテラシー向上に寄与していることがわかる.つまり,目的であったセキュリティ意識向上とセキュリティ教育のサポートを目的としたシミュレーションの開発を達成したといえる.本シミュレーションでは,攻撃と防御の両方の視点からシミュレートすることで効率的に学習することが可能となる.実際に攻撃や防御を体験することによって,学習意欲が高まり,より深い理解につながっていると考えられる.

6.2 今後の課題

アンケートの結果でもあったように,本シミュレーションは攻撃方法や防御方法が限られていることが課題点として挙げられる.より現実に近いシミュレーションを完成させるには,攻撃の種類を増やし,より多様化する必要がある.加えて,攻撃の被害や取得されたデータを視覚的に確認できるようにすることで,ゲーミフィケーションとしての価値がさらに高くなると考えている.

参考文献

[1] 国立研究開発法人情報通信研究機構” NICTER 観測レポート 2023”
https://csl.nict.go.jp/report/NICTER_report_2023.pdf, (参照 2025-07-24).

[2] NTT ビジネスソリューションズ ”巧妙化するサイバー攻撃の最新事情　「ランサムウェア」と「Emotet」に注意を　”
https://www.nttbizsol.jp/knowledge/security/2023022711000008 22.html ,(参照 2025-07-24)

[3] NRI SECURE ”NRI Secure Insight 2023”
https://www.nri-secure.co.jp/hubfs/NRIS/download/ebook/NRISecure_Insight2023_h8ut.pdf,(参照 2025-07-24)

[4] NRI SECURE ”セキュリティ人材不足の本当の理由”
https://www.nri-secure.co.jp/blog/reason-cybersecurity workforce-shortage,(参照 2025-07-24)

[5] 竹下数明,小林偉昭,佐々木良一：脆弱性対策教育のための e ラーニングシス テムの開発と評価　情報処理学会シンポジウム論文集,2009,pp439-444

[6] サイバー犯罪に関する白浜シンポジウム”情報危機管理コンテスト”
https://sccs-jp.org/symposium28/cmc19/cmc/ ,(参照)

[7] enPiT ”産業界が求める実践セキュリティ人材を育成”
https://www.enpit.jp/admission/security.html ,(参照)