「マルチメディア，分散，協調とモバイル
(DICOMO2021) シンポジウム」 令和3年6月-7月

試行錯誤を可能とするセキュリティ演習システムの提案

竹原 一駿[1]　石塚 美伶[1]　喜田 弘司[1]　最所 圭三[1]

概要：サイバー攻撃の高度化により，セキュリティの重要性が高まりつつあるが，日本では，セキュリティ人材の圧倒的な不足が報告されている．大学などの教育機関では，攻撃者からのサイバー攻撃を防御し，攻撃を発見した際に的確に対処するための知識と技術を持ったセキュリティ人材の育成が求められている．本研究では，セキュリティ人材の育成には，防御手法の自発的な調査，有効性を考えた選別，それらを活用した試行錯誤，が必要だと考え，サイバー攻撃に対する防御演習を試行錯誤できるシステム “ぷろてっくん” を提案する．本システムを用いることで，受講者は，任意の時点でセーブ&リストアができ，様々な防御手法の試行錯誤を可能とする．また，本システムは，単独での宿題型演習を想定しており，演習を行う受講者の全員が防御に関する技術を習得できる．演習は，防御した結果のスコアを用いたコンテスト形式とすることで，受講者により多くの試行錯誤を促す．本論では，セキュリティ人材の育成に必要な演習の内容の検討，“ぷろてっくん” を用いた宿題型コンテスト形式の防御演習の提案，本システムの特徴，本システムの持つ機能や構成の設計について述べる．

Proposal of a Security Exercise System Enabling Trial and Error

ICHITOSHI TAKEHARA[1]　MIREI ISHIZUKA[1]　KOJI KIDA[1]　KEIZO SAISHO[1]

1. はじめに

近年，コンピュータの多様化によりサイバー攻撃は日々高度化している．令和元年度の情報通信白書による企業の情報セキュリティに関する実態調査では，日本ではサイバーセキュリティ人材が圧倒的に不足していることが報告されている [1]．不足している人材の例としては，「ログを監視・分析して危険な兆候をいち早く察知できる」や「セキュリティインシデントへの対応・指揮ができる」が挙げられる．これらの人材を育成するための課題として，「キャリアパス (経験) の不足」が挙げられる．これらを受けて大学などの教育機関では，攻撃者からのサイバー攻撃を防御し，攻撃を発見した際にいち早く察知し，的確に対処するための知識と技術を持ったセキュリティ技術者の育成が求められる．また，IPA のアンケート調査によると，「今後身につける必要のある知識」として「情報セキュリティ」と回答する技術者が最多である [2]．これを受けて，IPA の情報処理技術者試験においても，セキュリティに関する出題割合を拡充しており，試験に合格することが，セキュリティに関する能力の指標となっている．

本研究では，大学などで育成された受講者のスキルレベルを，IPA にて提言される「共通キャリア・スキルフレームワーク」[3] に当てはめ，「基礎的知識を有し，要求された作業の指導を受けて遂行できる」(レベル 1，IT パスポート合格) と捉え，1 つ上の「要求された作業の一部を独力で遂行できる」(レベル 2，基本情報合格) への引き上げを目指す．資料 [3] による「スキル」とは「知識を活用して成果を生み出す能力」であり，スキルレベルの向上には知識の習得と活用が必要である．「知識」は，学習することで一定の範囲で身につくものであるが，即座にスキルに直結し成果が発揮されるものではない．これに対し，「スキル」は知識を活用し，実際にプロジェクト等の経験を重ねることで体得されるものである．即ち，受講者は，スキルレベルの向上を目指すことで，十分な知識と経験を得ることができ，セキュリティ人材育成に繋がる．

スキルレベルの向上は，以下を実践することで得られると考えた．

防御手法の調査 (調査)　防御手法の知識の習得である．サ

[1] 香川大学
Kagawa University

イバー攻撃に対する防御手法の自発的な調査が必要である．機器に異常を見つけたとき，ログや機器の設定を基に Web などを活用し，攻撃の原因や影響などを調査し，知識として習得する．

防御手法の選別 (選別) 習得した知識の活用である．防御手法の有効性はその時々で異なるため，得られた知識を基に機器に応じた，最適な手法の選別が必要である．例えば，機器の OS が異なれば，同じ防御手法を適応できないことがあり，機器の OS に応じた防御手法を選別しなければならない．

防御手法の試行錯誤 (試行) 防御手法において経験を重ねる．上記にて，調査し選別した知識を基に，攻撃に合わせた防御演習を実践する．同じ環境に対して，同じ攻撃の経験を重ねるだけでは，手順の暗記を繰り返すだけである．実際の業務において，スキルレベル 2 の「要求された作業」は要求毎に異なるので，暗記した内容を繰り返すだけでは，「独力で遂行できる」とは言いづらい．そこで，様々な環境における防御手法の実施による試行錯誤が，必要である．受講者が知識に基づき選別した防御手法でも，攻撃に対して必ずしも最適な防御手法とは限らない．様々な防御手法を試行錯誤することで，防御の成功や失敗を検証し，最適な防御手法を得ることの経験を重ね，今後の攻撃を見据えた防御を行える．このように，受講者に防御手法を試行錯誤させることで，次回の成功を目指すための更なる調査や選別を促す．

我々は，上記の，知識を活用した試行錯誤を促すために，サイバー攻撃に対する防御演習を試行錯誤できるシステム “ぷろてっくん”(Protec-kun(“kun” maens Mr.)) を提案する．受講者は，状況に合った最適な防御手法の実践のために，“ぷろてっくん” を用いて，調査と選別を行うことで知識の習得と活用を行う．得られた知識を基に演習を試行錯誤しながら繰り返すことで，経験を重ねスキルレベルの向上，ひいてはセキュリティ人材の育成に寄与すると考えている．

2. 関連研究

2.1 インシデントの仕組み学習と体験を可能とするセキュリティ訓練システム

清時らは，組織で起こるセキュリティインシデントの再発防止を目指し，組織の構成員で IT 技術に精通していない人物を対象に誘導型攻撃を学習，体験できるセキュリティ訓練システムを開発している [4][5]．当該論文における，セキュティ訓練システムの要件を，以下に示す．

- 組織で起こった Web を介す誘導型攻撃やランサムウェアなど，シナリオに応じたインシデントを再現できる．
- 個人に状況を判断，端末を操作させ，その結果として何が起こるか体験できる．
- 機器の操作の結果，起こった個々の事象について説明できる．

受講者は，攻撃対象の機器へ遠隔ログインし，シナリオに応じた訓練を実施する．一例として，ランサムウェア [6] のシナリオを用いた学習について述べる．システムが用意した Web サイトで悪意のある広告をクリックすると，脆弱性への攻撃が行われ，ランサムウェアがダウンロード，実行される．実行と同時に，PC 内のファイルが暗号化され，金銭を要求するメッセージが示される．以上のシナリオにより，安易に広告をクリックしないことが学習できる．シナリオでは，受講者が攻撃を受ける行動 (ランサムウェアのダウンロードなど) に注目しており，あくまで受講者が能動的に行動しないと攻撃されない．訓練実施前後に行なった評価では，12 名を対象に，IT パスポート試験を参考に 10 問出題し，演習実施後に平均正答数が 2~3 問増えた．

これにより，当該論文の訓練システムにより，演習環境内で，能動的に攻撃を受け，攻撃の結果を体験することで，知識を増やせると言える．

2.2 体験型サイバーセキュリティ学習システム

八代らは，体験型学習は，座学よりも高い学習効果が得られるがインストラクターを必要とすることが多いことに着目し，初学者を対象に自習形式でセキュリティを体験学習できるシステムを提案している [7][8]．初学者は，セキュリティの基礎的知識及び，Linux や Windows の基本操作を身につけている者，と定義している．当該論文の提案システムは，Linux や Windows の機器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を提供する学習支援システムの，2 部で構成される．受講者は，まず，演習に必要な知識の習得を学習支援システムで獲得する．次に，その知識を使って，演習環境上でログの参照や検索を行う．最後に，演習内容の理解を確認するために，演習後に，学習支援システムにて確認テストを行う．確認テストは，学習支援システムにて自動採点されるため，受講者は，インストラクターの支援を必要としない．訓練実施前後に行なった評価では，33 名を対象に，情報処理技術者試験などの公的試験を参考に 10 問出題し，演習実施後に平均正答数が平均 2~3 問増えた．

これにより，体験型演習であっても，インストラクターが不在である自習形式での演習が実現でき，学習効果が確認できることが言える．

2.3 MicroHardeing

(株) 川口設計 [9] は，「MicroHardening」を開発している．MicroHardeing は，4 人 1 組のグループで，クラウド上に構築した EC サイトを提供する Web サーバを，様々な攻撃から守る競技である．サイバー攻撃への対応のために役割分担を行い，対応記録の整理や情報共有など技術外

の対応も含めて演習できるとしている．演習形式は，45 分間の演習セットを複数回繰り返す．毎回同じタイミングで同じ攻撃がやってくるため，繰り返しの中でシステムの防御方法を学ぶことができる．

“ぷろてっくん” と同様に，学習した知識は，演習の繰り返しの中で定着することを提言している．同じタイミングで同じ環境に対して同じ攻撃がくるため，受講者は，MicroHardening のみに対する防御手法を実践する．しかし，グループでの競技であるため，技術力の高いメンバーが機器の操作や調査を全て行なってしまい，技術力の低いメンバーは置き去りになることが多い．そのため，不足している人材である，ログの監視やセキュリティインシデントへの対応ができる人材が，MicroHardening の演習ではグループの特定のメンバーに限定される．

また，MicroHardeing は，あくまで通常のエンジニアに対し，セキュリティを「ちょっと」知ってもらうことを念頭においており，セキュリティ専門家の育成を対象にしておらず，1 章で述べたセキュリティ人材の育成には，力不足である．

3. “ぷろてっくん” を用いた演習の想定

演習は，コンテスト形式で行い，防御演習を一定期間毎に防御スコア (4 章にて後述) を受講者同士で比較する，受講者は，調査や選別に長い時間取り組むため，宿題型の演習とする．コンテスト形式は，プログラミング演習 [10] や多くの大会において導入されている．有名なところでは，国際プログラミングコンテスト “ACM-ICPC”[11] や “AtCoder”[12] がある．近年では，チューニングによるサービスの高速化を目的としたコンテスト “ISUCON”[13] もある．コンテスト形式は，ゲーム感覚のイベントで参加でき，良い成績を得るという目的意識が明確になる．また，受講者同士で対抗意識や挑戦意欲による学習効果の向上が期待できる．“ぷろてっくん” を用いた演習においてもコンテスト形式を用いることで，より多くの試行錯誤を促す．

受講者は，スキルレベル 1 と想定し，基礎的知識である機器の操作 (コマンドなど) は，習得済みであるとする．

受講者は，図 1 の流れで防御演習を行う．まず，受講者に対して，以下の事前説明を行う．

機能説明　受講者に，防御スコアや試行錯誤の機能と，演習の流れを説明する．サービスが明確に攻撃を受けており，受講者が対応する必要があることを認知させる．

調査方法　攻撃を受けたときにどのファイルにログが出力されるか，ログを基にした Web の調査方法などを示す．実際に攻撃を受け防御する例示があると良い．防御演習で得た調査の方法などは，受講者間で共有することも説明する．

使用方法　受講者が防御する機器への自宅からのアクセス方法や，試行錯誤を行うためのセーブ&リストアの方法を説明する．

次に，受講者に，宿題の締切を 2 回用意する．受講者に，第 1 締切として，1 週間程度の自宅での防御演習を課す．受講者は，単独で調査や検討を繰り返しながら，試行錯誤を行い，防御スコアの継続的な向上を目指す．防御スコアは，他者と定期的に共有される．

第 1 締切終了後，受講生は，調査の方法やコツなどを共有することで，相互に知識を高め合う．例えば，自らが気づかなかった攻撃のログの出力内容や，攻撃に対する Web での検索ワードの良い選び方などである．共有は，防御演習に関するノウハウのみであり，実際の演習環境を用いる必要はなく，オンライン環境でも十分に共有できる．

これらの共有後に，第 2 締切として再び 1 週間程度の単独での防御演習を課す．共有により得られた他者の知見も活かし，更に新たな知識や経験を得る．このときの演習は，第 1 締切と同じ攻撃内容とする．ただし，第 1 締切のときとは異なる環境 (OS など) で演習する．第 1 締切までに得た知識と経験を活かし，他の環境での防御を目指す．自らより高い防御スコアを取得した学生を目指し，試行錯誤を行う．

最後に，防御スコアを比較することで，受講生がどの程度サービスを防御できる知識と経験を得たのか評価する．

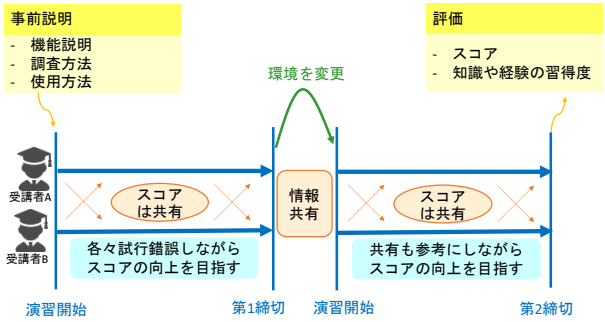

図 1　防御演習の流れ

4. “ぷろてっくん” の特徴

“ぷろてっくん” は，以下の特徴を持つ．

攻撃に対する防御を試行錯誤できる　演習システムを任意の時点でセーブ&リストアし，様々な防御手法を試行錯誤できる．1 つの攻撃に対して，攻撃に対する防御手法を何度も実践し，最適な防御手法を試行錯誤しながら習得できる．受講者は，今後，重要になると考えたタイミングでセーブし，セーブポイントを記録できる．例えば，攻撃を開始された直後などである．攻撃に対する防御手法を実践する．その後，セーブポイントを選択することで攻撃開始の直後にリストアし，異なる防御手法を実行できる．

演習における試行錯誤の例を示す (図 2)．攻撃を受け

ており防御前の状態をセーブ (A) する．場当たり的にポートの全遮断を行う．その結果をセーブ (B) する．次に，(A) をリストアし，よく攻撃が行われる Telnet ポートを遮断しセーブする (C)．同様に HTTP を遮断しセーブする (D)．このように異なる手法を試行し，各セーブで最も防御スコアが高い手法を選別する．

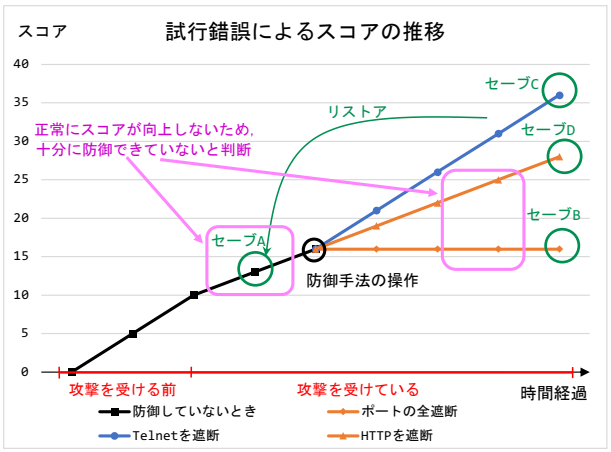

図 2　試行錯誤パターン

異なる環境での防御を実践できる　攻撃に対し，異なる環境 (OS やアプリケーションなど) での防御を実践できる．同じ攻撃かつ同じ防御方針であっても，環境が異なると操作する内容は異なる．自らの持つ知識から，環境に合った防御手法の選別を促すことができる．

単独で演習できる　受講者は，他者を必要とせず単独で演習することができる．単独による演習を行うことで，攻撃から防御するための調査や操作など，防御手法において手を動かす操作を経験できる．自らが操作した結果の状況を自らで学ぶことで，レベル 2 の要件でもある作業の独力での遂行を目指す．関連研究の MicroHardening(2.3 節) などの，グループワークによる演習では，メンバーの連携による即座な対処が求められる．そのため，機器の現状の調査や防御の適応を，メンバーの技術力が高い 1 人が独占してしまい，全ての操作を終えてしまうことがある．その結果，他メンバーは行った操作の意味を理解せず，他メンバーのスキルレベルの向上に寄与しないこともある．単独による演習で，受講者は防御に関する (手法の調査や機器の操作など) 実践的な技術を身につけることができる．

自宅で演習できる　受講者は，システムにオンラインでアクセスすることで，自宅で防御演習を行える．宿題型の自宅演習とすることで，防御手法の調査や試行錯誤の検討に，長時間かけて取り組むことができる．より最適な防御手法の模索のために，試行錯誤を繰り返すことができる．また，昨今ではオンライン講義が増えており，グループワークなどの他者を必要とする演習の機会が減りつつある．そのような場合でも，自宅でオンライン演習を行うことで，受講者のスキルレベルを向上させる．

受講者は実際に機器を操作する　受講者は，サービスを提供し，攻撃を受ける機器を操作できる．コマンド操作を行い，ログを実際に調査し，攻撃の種別や防御手法を検討し，機器に対して手法を実行する．環境に合った，新たな防御手法の調査と，知識の習得を促す．

防御の度合いがわかる　攻撃に対する防御を実践した結果，どの程度成功しているかをスコアで示す．受講者は，スコアの推移を確認できる．スコアは，他の受講者とも共有され，他者との対抗意識を促す．例としては，提供サービスが EC サイトならば，サービスに対する継続的な売上が防御スコアとなる．受講者は，自らが実践した防御手法が効果的であるか判断でき，試行錯誤しながら高い防御スコアの取得を目指す．本スコアにて，スキルレベルが向上したと言える指標は，受講者が環境に合わせた完璧な防御を行なったときの，6 割程度だと考えている．これは，攻撃に対する防御の操作を「要求された作業」と捉えると，基本情報技術者試験の合格点数である 60 点 (100 点満点) 程度が指標であると考えたためである．

5. ぷろてっくんの設計

5.1 システムの機能

“ぷろてっくん” は，以下の機能を持つ．

標的機能　受講者が防御すべきサービスを提供する．サービスの防御のために，防御手法を自発的に調査する．サービスの例として，EC サイトやファイル共有が挙げられる．

攻撃機能　受講者の防御する “標的機能” を攻撃する．サービスを提供する機器にバックドアを仕掛けたり，サービス自体の脆弱性を狙った攻撃を行う．また，ユーザリストなどのサービスの運営に関わるデータを奪取し，それを基にした攻撃を行う．

防御スコア機能　受講者がどの程度システムを防御できているか示す．受講者は，他の受講者と共有された防御スコアの推移を確認できる (図 3)．サービスにアクセスし，正常に提供されているか確認する．正常ならば攻撃を受けておらず，防御スコアは上昇する．時間が経過しても，防御スコアが思うように上昇していないときは，攻撃を受けており，防御が失敗している．

環境変更機能　サービスを様々な環境 (e.g. Linux / Windows, Apache / Nginx) で提供する．

状態管理機能　システムの任意の状態をセーブ&リストアする．防御スコアや攻撃機能もセーブされ，任意のセーブポイントでリストアできる．状態は Snapshot を用いてセーブし，木構造で管理する．

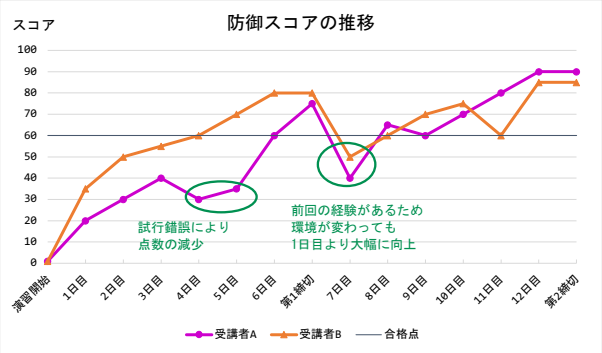

図 3　防御スコアの推移

単独演習機能　受講者に，機器の操作を提供する．SSH などを用いて遠隔ログインし，機器に対し，ログの確認や防御手法の操作ができる．ログを実際に調査し，攻撃の種別や防御手法を検討し，機器に対して手法を実行する．

自宅演習機能　オンライン環境で機器や状態管理機能を操作できる．会場を必要とせず自宅のオンライン環境で演習できる．

5.2　システムの構成

本節では，演習の一例として，EC サイトのサービスを防御する演習を行うときの，“ぷろてっくん” の構成について述べる．図 4 に “ぷろてっくん” の全体構成を示す．本システムでは，受講者は，サービスの防御に，サービスを提供する EC 部を操作する．EC 部で提供されているサービスは，PURCHASE 部より防御スコアの確認処理が行われる．ATTACK 部より攻撃が行われるため，EC 部を操作し防御しなければならない．MSR 部では，上記の 3 部を操作できる．受講者には，防御スコアの推移の表示，EC 部へのコマンド操作，MSR 部の Web 画面での操作，を提供する．これらは，単独で全てにアクセスでき (単独演習機能)，インターネットを通じたオンライン環境により自宅からでもアクセスできる (自宅演習機能)．

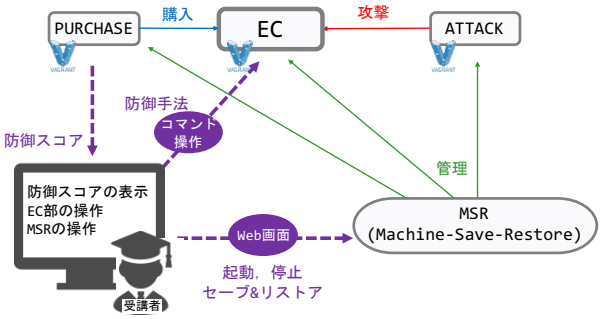

図 4　ぷろてっくんのシステム構成

各部について述べる．

PURCHASE 部　EC 部に対し，Bot として購入処理を行う (防御スコア機能)．購入処理に成功すると，防御スコアが上昇する．購入処理は一定に行われるため，攻撃を受けているときは購入処理が成功せず，防御スコアが思うように上昇しない．

EC 部　サイバー攻撃を受けるための脆弱な状態のサービスを提供する (標的機能)．PURCHASE 部からの ID とパスワード認証を有した PURCHASE 処理を受け取る．受講者は，SSH などを用いて遠隔ログインし，ログの確認や防御手法の操作ができる．また，EC 部でのサービスは様々な環境で構築される (環境変更機能)．

ATTACK 部　PURCHASE 部に対して攻撃を行う (攻撃機能)．サービスの脆弱性を利用した攻撃 (SQL インジェクションなど) や，SSH の不正ログインによるユーザリストの奪取などを行う．また，パスワードの総当り攻撃なども行うため，一見侵入されていなくても，安全とは言えない．

MSR(Machine Save Restore) 部　一元的に EC 部，PURCHASE 部，ATTACK 部を操作する (状態管理機能)．命令は，システムの起動，システムの停止，システムのセーブ，システムのリストアである．受講者は，MSR 部が提供する Web 画面にアクセスすることで，木構造でシステムの Snapshot をセーブしたり (図 5)，再度試行したいセーブポイントにリストアできる (図 6)．

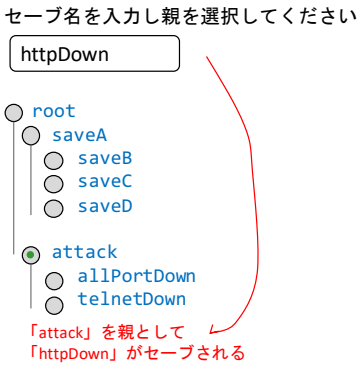

図 5　Snapshot のセーブ選択画面例

6.　おわりに

大学では攻撃を防御し，発見し，対処する知識と技術を持ったセキュリティ人材の育成が求められている．本研究では，大学の受講者のスキルレベルを「要求された作業の一部を独力で遂行できる」への引き上げを目指している．スキルレベルが向上することで，十分な知識と経験を得ることができ，セキュリティ人材が育成できる．我々は，防御演習を試行錯誤しながら行うことで，セキュリティ教育におけるスキルレベルが向上すると考え，受講者が防御演習を試行錯誤できるシステム “ぷろてっくん” を提案した．

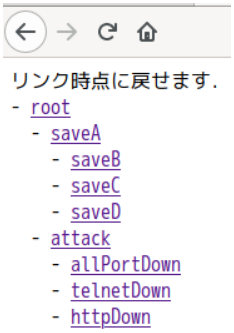

図 6 Snapshot のリストア選択画面例

試行錯誤を行うことで，防御に関する知識の習得，活用を得て，経験を重ねることができる．本システムは，自宅での宿題型のコンテスト形式で使用することで，より多く試行錯誤を目指す．受講者は，単独で演習を行うことで，受講者は必ず防御に関する実践的な技術を身につけることができる．

今後は，“ぷろてっくん” の開発と学生を対象にした評価を行う．

参考文献

[1] 総務省, “総務省 — 令和元年版情報通信白書 —サイバーセキュリティに関する現状と新たな脅威”. https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/html/nd113310.html, 2021/05/04.

[2] IPA 独立行政法人 情報処理推進機構, “プレス発表 i パス（IT パスポート試験）をはじめとする情報処理技術者試験の出題構成の見直しについて”. https://www.ipa.go.jp/about/press/20131029.html, 2021/05/09.

[3] IPA，“共通キャリア・スキルフレーム (第一版・追補版)”. 独立行政法人情報処理推進機構 IT 人材育成本部 IT スキル標準センター，pp.7，2012/06/17.

[4] 清時耀, 福田洋治, 井口信和, “インシデントの仕組みの体験学習を可能とするセキュリティ訓練システムの開発 -情報収集作業を支援する訓練シナリオ作成機能の検討-”. 2019 年度 情報処理学会関西支部 支部大会 講演論文集, G-08, 2019.

[5] 清時耀, 福田洋治, 井口信和, “インシデントの仕組み学習と体験を可能とするセキュリティ訓練システムの開発 -Web を介した誘導型攻撃の訓練の評価と確認テストの機能の検討-”. 第 81 回全国大会講演論文集 pp.411–412. 2019.

[6] トレンドマイクロ, “ランサムウェア — トレンドマイクロ”. https://www.trendmicro.com/ja_jp/security-intelligence/research-reports/threat-solution/ransomware.html, 2021/05/09.

[7] 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 論文集, pp.1453–1460, 2017.

[8] 八代哲, 田邉一寿, 齋藤祐太, 齋藤孝道, “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”. マルチメディア, 分散協調とモバイルシンポジウム 2018 論文集, pp.1809–1816, 2018.

[9] 株式会社 川口設計, “MicroHardening”. https://www.sec-k.co.jp/mh, 2021/05/09.

[10] 富永浩之, 太田翔也, “実行テスト系列を取り入れた小コンテスト形式の初級 C プログラミング演習における段階的実装を誘導する得点ルール”. 情報教育シンポジウム論文集, 2017(33), pp.206–211, 2017.

[11] ICPC, “国際大学対抗プログラミングコンテスト”. https://icpc.iisf.or.jp/, 2021/05/09.

[12] AtCoder, “競技プログラミングコンテストを開催する国内最大のサイト”. https://atcoder.jp/, 2021/05/09.

[13] ISUCON, “公式 Blog”. https://isucon.net/, 2021/05/09.