情報セキュリティ対策のおける疑似体験型 Web テストの開発と選択肢列挙タイプ e-learning 確認テスト結果との比較

松澤 英之

宮崎大学 情報基盤センター

matuzawa@cc.miyazaki-u.ac.jp

Development of Simulated Experience Web Test about Information Security Measures and Comparison with Results of Web Test and Conventional E-learning Test

Hideyuki Matsuzawa

Information Technology Center, University of Miyazaki

概要

情報セキュリティ対策講習に関して e-learning でよく用いられる回答選択肢列挙型タイプ確認テストの学習効果を調べる為に、ユーザが実際に使用するソフトウェアの画面イメージを用いた疑似体験型 Web テストを開発してその結果を比較する。

1 はじめに

日本でのインターネットの普及により時間と場所の制約を受ける対面での講義ではなく e-learning が用いられる事が多くなっている。e-learning は最初に Web 上の教材で自習、次に自習内容についての確認テストを行うパターンが多い。昨今企業のコンプライアンスが強く求められているので教育の一環として場所と特に時間にとらわれずに受講出来る e-learning が用いられていることが多い。

宮崎大学でも e-learning を用いて情報セキュリティ対策についての講習、確認テストを 3 年前から行っている。この情報セキュリティ対策講習は昨年度までは教職員と大学院生(留学生を含む)を対象に行っていたが、本年度から学部学生(留学生を含む)も対象に含まれるようになった。今年度の情報セキュリティ対策講習は最初に 2018 年度速習版 INFOSS 情報倫理[1]を受講、次に講習内容に沿った確認テスト 25 問に回答する。この確認テストは宮崎大学情報基盤センターが作成している。受講者が全問正解するとその年度の宮崎大学統一認証 ID の利用が許可される。宮崎大学統一認証 ID は大学が提供している様々な Web サービスの認証に利用されている。確認テストはある課題に対して 3-4 個の選択肢から正解を選ぶ形式である。再受験しても問題と選択肢の内容は変わらないが、受験するたびに問題と選択肢がランダムな順番で表示される。

では全学で行われるこの情報セキュリティ対策講習はユーザがパソコンを使う際に情報セキュリティ対策としてどの程度役に立たつのであろうか。情報基盤センターとしては講習の効果測定は行っていない。そこで個人的に院生、学部学生に聞いたところ確認テストで全問正解しても実際の情報セキュリティ対策には役に立たないのではないかという意見が殆どであった。非常に狭い範囲の意見収集ではあるが情報セキュリティ対策において従来型の e-learning 講習、確認テストが実際の情報セキュリティ対策の向上に役立っているか疑問があり、確認する必要があると考えた。

まずユーザがパソコンを利用する際にどの程度情報セキュリティ対策を行えているのか測定する必要がある。今回は実際に使われているパソコンでの情報セキュリティ対策を観測するのではなく、実際のパソコン使用環境(ソフトウェア利用画面)を模した疑似体験環境を利用した Web テストを開発し情報セキュリティ対策の実情を観測することとした。次に従来型の選択肢から正解を選ぶ選択肢列挙タイプ e-learning 確認テストと開発した疑似体験型 Web テストの結果を比較することで情報セキュリティ対策における従来型 e-learning の有効性を確認する。

2 従来型回答選択肢列挙タイプ e-learning 確認テスト

従来型 e-learning では情報セキュリティ対策ごとに講習と確認テストを行っているものが多い。また日々新しい情報セキュリティインシデントが発生しそれに対する対策が練られているので、個別の情報セキュリティ対策毎に解説をすることで既存の e-learning 講習全体の構成をそれほど変更することなく簡単に新しい解説内容を付け加えることができる。

ただしこの様な講習の構成は情報セキュリティ対策を実践させるあるいは解説を行う側には都合がよいもので、ユーザがパソコンを使用する時に情報セキュリティ対策を行えるように作られているとは言い難いと考える。そこで実際に情報セキュリティ対策に詳しい人々がどのように情報セキュリティ対策を行っているか具体的に考えてみた。例えば電子メールを受け取った場合ユーザはまず電子メールソフトウェアが表示する画面で情報セキュリティ対策上判断に必要な箇所を見つけ出し、次に見つけた箇所の画面情報から安全であるか否かを判断している。つまり最初にソフトウェア画面上で情報セキュリティ対策を行う上で判断に必要な部分(注目点)を見つけていることになる。情報セキュリティ対策上の注目点について従来の e-learning でも解説文の中でわずかながら説明されている。一般に解説者が強調したい部分あるいは受講者の理解が難しい部分は理解・記憶を促進するために図解されることが多いので解説文だけの情報セキュリティ対策上の注目点は受講者の意識に残っていないかユーザが重要だと認識していないのではないかと考える。例えば 2018 年度速習版 INFOSS 情報倫理のフィッシング詐欺では解説が 15 行記述されているが、その中でフィッシング詐欺に遭わないための電子メール本文の注目すべき部分について約 2 行しか記述されていない。

3 疑似体験型 Web テスト

ユーザがパソコンを利用する際にどの程度情報セキュリティ対策を行っているか計測するためにユーザが実際に使用しているソフトウェア画面を利用した疑似体験型 Web テストが必要になると考える。これは先に述べた情報セキュリティ対策に詳しい人が日々行っている行動をトレースするテストであるともいえる。

疑似体験型 Web テストは 2 段階からなる。第 1 段階は 使用しているソフトウェア(電子メールソフト、Web Browser 等)が表示するディスプレイの画面イメージの中で情報セキュリティ対策において注意を払わねばならない画面イメージ部分を選択する、第 2 段階は第 1 段階で選択した画面イメージ部分に対してとる行動を選択させる設問に答える。第 1 段階は IPA のフィッシング(Phishing)対策におけるフィッシング事例(2004 年 11 月)[2]、標的型攻撃メール<危険回避>対策のしおり[3]5 ページのイメージ画像に近い。第 2 段階の部分は従来型回答選択肢列挙タイプの e-learning 確認テストと同じ形態となる。

第 1 段階で画面イメージのどの部分に注意を払うかという設問は設問対象となっている画面イメージ部分(正解領域)をクリックすることによって回答する。設問は画面イメージのすべての領域に設けられているわけではない。第 2 段階の設問への移動は当該画面イメージ部分に設定されたクリッカブルマップをクリックすることで行われる。クリッカブルマップは html 言語の img タグ、map タグ、area タグで作成される。クリッカブルマップのリンク先に第 2 段階の設問を表示する画面を設定する。リンクの設定は area タグの href 属性を利用している。クリッカブルマップのデフォルト設定ではクリッカブルマップ上にポインタを動かすとアイコンイメージが変化する。つまりデフォルトの設定では出題された画面イメージ上で適当にポインタを動かしているとポインタイメージの変化によって回答すべき領域が回答者にわかってしまう。ポインタが変化する事の可否はここでは述べないが、今回は area タグのスタイル属性である"cursor"属性を"default"に指定してクリッカブルマップ上にポインタが来てもポインタイメージが変化しない仕様にした。Internet Explorer、Edge はこの"cursor"属性が有効にならないので、img タグのスタイル属性である"cursor"属性を"default"にして同じ効果を出している。この設定によって画面イメージ上でポインタを動かしただけでは回答すべき部分を判別することができない。この設定によって回答の難易度は確実に増加する。ただしリンクポイントにポインタ

を置いた時ブラウザ欄外にリンク先 URL が表示されるあるいは一部のブラウザでクリッカブルマップの境界が破線で表示されることを利用してクリッカブルマップの存在を見つけることはできるが、この表示変化に初心者は気が付かないと思われるので今回は特に対処しない。

これ以外にも回答の難易度を上げる仕掛けとして情報セキュリティ対策とは関係なく第 2 段階の選択肢のどれを選んでも正解にならないダミー領域(不正解領域)を設けた。これにより問題イメージをやみくもにクリックして正解領域を判別する行為を防いでいる。

図 1、図 2 に第 1 段階の疑似環境の作成時に用いた画像イメージを示す。図 1 は電子メール、図 2 は Web ブラウザについての問題イメージである。実際出題される際は表示されないが正解領域は青枠で、不正解領域は赤枠で示してある。

今回作成した問題は以下の通り。

1. 電子メール

図 1　電子メール

問題で用いた電子メールの画面イメージは実際に私に送られてきた電子メールを少々改変して使用した。この画面イメージは宮崎大学が提供している Web メールソフト DEEPMail[4]から取得した。

問題文

電子メールについての問題です。貴方に見知らぬ送信者 "管理者<ikegami@illum**.jp>" からメールが届きました。 情報セキュリティ上注目しなければならない点を画像上でクリックしてください。設問が表示されます。

全ての着目点で回答した時点で回答ボタンをクリックしてください。

(設問が表示される領域には不正解の領域(どの回答も全て不正解) も含まれています)

第 2 段階の設問

問題(1) 送信者に対する問題です。間違っている対応を一つ選びなさい

1. 知らない人からの電子メールであるが特段気にしない。
2. 知らない人からの電子メールであるのでメールを無視する。
3. 知らない人からの電子メールであるので十分注意して本文、リンク先、添付ファイルを扱う。

(正解は 1)

問題(2) 宛先に対する問題です。間違っている対応を一つ選びなさい

1. 自分宛ではないのでメールを無視する。
2. 自分宛ではないので十分注意して本文、リンク先、添付ファイルを扱う。
3. 自分宛ではないが特別注意を払わない。

(正解は 3)

問題(3) 件名に対する問題です。間違っている対応を一つ選びなさい

1. 関係のない用件であるが注意してリンク先、添付ファイルを扱う。
2. 件名について特段気にしない。
3. 関係のない用件あるのでメールを無視する。

(正解は 2)

問題(4) 添付ファイルに対する問題です。正しい対応を一つ選びなさい

1. 添付ファイルをダウンロードしてウィルスチェックをする。
2. 添付ファイルが実行ファイルなのでダウンロードしない。
3. 添付ファイルを開くように書いてあるのでダウンロードして開封する。

(正解は 2)

問題(5) リンク先に対する問題です。間違っている対応を一つ選びなさい

1. とりあえずホームページを開いてみる。
2. ホームページがどのようなところか調べてみる。

3. 署名の電子メールアドレス、送信者、リンク先のホームページを比較する。一致する場合だけホームページを開く。

(正解は 1)

問題(6) 署名に対する問題です。正しい対応を一つ選びなさい

1. 署名の電子メールアドレスに特段注意を払わない。
2. 署名の電子メールアドレス、送信者、リンク先のホームページを比較し一致しない場合は信用しない。
3. 署名の電子メールアドレス、送信者、リンク先のホームページを比較し一致しなくても添付ファイルの開封、リンク先を参照する。

(正解は 3)

問題(7) 個人情報に対する問題です。間違っている対応を一つ選びなさい

1. 不必要な個人情報を送信していないか確認する。
2. パスワードを送信していないか確認する。
3. 記載する情報が正しい事を確認する。

(正解なし)

問題(8) 本文 1 に対する問題です。間違っている対応を一つ選びなさい

1. 本文の内容について自分に関係のある内容かよく吟味する。
2. 本文の内容にかかわらず添付ファイルをダウンロードする。
3. 本文の内容にかかわらずリンク先にアクセスする。

(正解なし)

問題(9) 本文 2 に対する問題です。間違っている対応を一つ選びなさい

1. 本文の内容について自分に関係のある内容かよく吟味する。
2. 本文の内容にかかわらず添付ファイルをダウンロードする。
3. 本文の内容にかかわらずリンク先にアクセスする。

(正解なし)

問題(10) 本文 3 に対する問題です。間違っている対応を一つ選びなさい

1. 本文の内容について自分に関係のある内容かよく吟味する。
2. 本文の内容にかかわらず添付ファイルをダウンロードする。
3. 本文の内容にかかわらずリンク先にアクセスする。

(正解なし)

2. Web ブラウザ

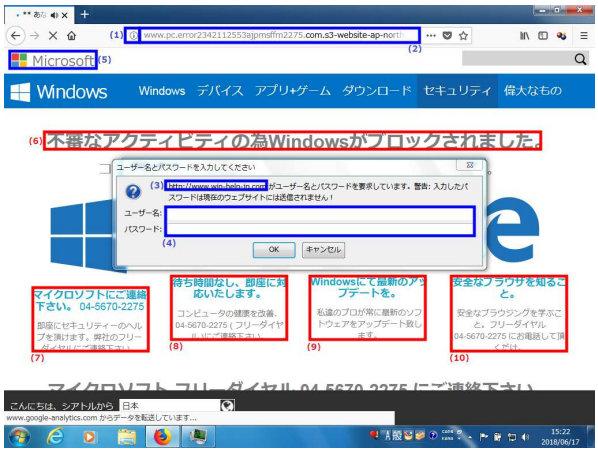

図 2 Web ブラウザ

Web ブラウザ FireFox[5]の画面イメージは実際に私が遭遇したブラウザ画面を少々改変して使用した。

問題文

ホームページ閲覧についての問題です。貴方があるホームページを見ている突然以下のホームページが開きました。 情報セキュリティ上注目しなければならない点を画像上でクリックしてください。設問が表示されます。

全ての着目点で回答した時点で回答ボタンをクリックしてください。

(設問が表示される領域には不正解の領域(どの回答も全て不正解)も含まれています)

第 2 段階の設問

問題(1) 接続方法に対する問題です。正しい対応を一つ選びなさい

1. 認証局の情報を当てにしないで接続する。
2. 認証局によって認証されていないが一般のホームページでも認証されていないホームページが多いので気にせず閲覧する。
3. 認証局によって認証されていないので注意して閲覧する。

(正解は 3)

問題(2) 接続先に対する問題です。正しい対応を一つ選びなさい

1. ユーザ名・パスワード入力欄に記載されている URL と異なるが閲覧を続ける。
2. ブラウザの URL、ユーザ名・パスワード入力欄に記載されている URL が Microsoft のホームページとは関係ないので今すぐ閲覧をやめる。
3. Microsoft のロゴがあり Microsoft のホームページと思われるので閲覧を続ける。

(正解は 2)

問題(3) ユーザ名、パスワード入力欄の接続先に対する問題です。間違っている対応を一つ選びなさい

1. ブラウザの URL、ユーザ名・パスワード入力欄に記載されている URL が Microsoft と接続先のホームページは関係ないので接続しない。件名について特段気にしない。
2. Microsoft のホームページと思われるので接続する。
3. ユーザ名、パスワード入力欄に記載されている URL と異なるが接続する。

(正解は 1)

問題(4) パスワードに対する問題です。間違っている対応を一つ選びなさい

1. ブラウザの URL、ユーザ名・パスワード入力欄の URL が異なるので入力しない。
2. どのユーザ名、パスワードかわからないので入力しない。
3. どのユーザ名、パスワードかわからないがとりあえず入力する。

(正解は 2)

問題(5) ホームページに対する問題です。間違っている対応を一つ選びなさい

1. Microsoft のホームページなので信頼して閲覧する。
2. ホームページ名、接続先の URL とユーザ名・パスワードの入力先が一致しないので今すぐに閲覧を止める。
3. 接続先の URL と Microsoft のホームページは関係ないので今すぐに閲覧を止める。

(正解は 1)

問題(6) タイトルに対する問題です。正しい対応を一つ選びなさい

4. 非常に重要なメッセージに見えるので信頼して閲覧する。
5. 閲覧中に現れた警告文に見えるので信頼して閲覧する。
6. Windows がブラックされたようなのでホームページの内容に沿って解決する。

(正解はなし)

問題(7) 本文 1 に対する問題です。正しい対応を一つ選びなさい

1. マイクロソフトに連絡するように書いてあるので、とりあえず電話してみる。
2. こちらの連絡先が分かるように電話してみる。
3. 電話番号がフリーダイヤルではないので電話しない。

(正解なし)

問題(8) 本文 2 に対する問題です。正しい対応を一つ選びなさい

1. 即座に対応してもらえるようなのでとりあえず電話してみる。
2. コンピュータの健康を改善してくれるようなのでとりあえず電話してみる。
3. 電話番号がフリーダイヤルではないので電話しない。

(正解なし)

問題(9) 本文 3 に対する問題です。正しい対応を一つ選びなさい

4. Windows をアップデートしてもらえるようなので連絡する。
5. アップデートが有料か無料化わからないのでその点を確かめる。
6. Windows のアップデートをしない。

(正解なし)

問題(10) 本文 4 に対する問題です。正しい対応を一つ選びなさい

7. 安全なブラウザを教えてもらえるので、連絡する。
8. 安全なブラウザを教えてもらっても解決しそうもないので連絡しない。
9. 教えてもらえる情報をきいてから判断する。

(正解なし)

比較実験を行う前に動作確認のために 2018 年度宮崎大学教育学部情報科学演習の受講者、教育学部 3 年生 3 名にテストを行ってもらった。その結果を踏まえて設問の画面イメージ以外に回答した領域を枠で囲った別の画面イメージを追加した。これによって回答者が同一領域を複数回回答することはなくなる。

4 比較実験

疑似体験型 Web テストは電子メールと Web ブラウザに対する問題を作成した。疑似体験型 Web テストとの比較のための従来型回答選択肢列挙タイプ e-learning 確認テストとして今回比較実験に参加した学生全てが受けている 2018 年度宮崎大学情報セキュリティ対策講習のテストのうち電子メールの利用に関連した確認テスト問題 2 問(過去問題)を出題した。テストの最後にアンケート調査を行った。対象は 2018 年度前期に私が講義を担当した宮崎大学教育学部情報・数量スキル E1、E3 受講者、教育学部 1 年生 84 人。今回はすべての設問に回答した学生のみ統計の対象としたので 84 人中 73 人から結果を得た。複数回問題に回答した場合は最後の回答を採用した。ちなみに 2018 年度宮崎大学情報セキュリティ対策講習のテストは 2018 年 5 月 8,9 日に情報・数量スキルの講義中に実施し、今回の比較実験は 2018 年 7 月 17,18 日に行った。

比較実験で出題した電子メールに関する 2018 年度宮崎大学情報セキュリティ対策講習のテストは以下のとおりである。

電子メールに関する対応のうち、適切なものを 1 つ選びなさい。

1 つ選択してください:

a. 海外から英文で DM が送られてきたので、本文中に書かれた URL をクリックしてみた。

b. 知らない人からコンピュータウィルスに関する電子メールが届いたが、無視した。

c. 覚えのないアドレスからメールが続けて届くようになったので、送信をやめてくれるよう返信した。

d. 差出人不明の電子メールに添付ファイルが付いていたので、確認のために開いた。

(正解は b)

電子メール利用の注意点として、適切なものを 1 つ選びなさい。

1 つ選択してください

a. 携帯電話からコンピュータにメールを送信する場合、携帯電話固有の絵文字や記号を使うとよい。

b. 電子メールを書くときには、1 文ごとに 1 行あけると読みやすくなる。

c. 電子メールを書くときには、HTML を活用して画像や文字装飾による豊かな表現をするように心がける。

d. 大きなデータを送信する場合、該当ファイルをサーバにアップロードしておき、その URL をメールで通知して、受信者にダウンロードしてもらう。

(正解は d)

アンケート内容は以下のとおりである。

・問 1 平成 30 年度情報セキュリティ対策講習で受講した問題について

適切な選択肢を覚えていましたか？

はい　　いいえ

・問 2 平成 30 年度情報セキュリティ対策講習で受講したメールの問題(第 1 問)と第 2 問で受講したメールの問題の内容について

・問 2-1 どちらの問題の方が記憶に残りますか？

第 1 問　　第 2 問

・問 2-2 どちらの問題の方が難しいですか？

第 1 問　　第 2 問

・問 2-3 どちらの問題の方が実際のパソコンを利用するうえで役に立つと思いますか？

第 1 問　　第 2 問

理由を記入してください(自由記述)

・問 3 第 2 問(Mail)と第 3 問(Web Browser)のような形式の問題は実際のパソコンを利用するうえで情報セキュリティについて習得或いは確認するのに有効だと思いますか？

●習得する為に

有効である、 有効ではない

●確認する為に

有効である、 有効ではない

アンケートの結果

問 1　はい=53.4%、いいえ=46.6%

問 2-1 第 1 問=50.7%、第 2 問 49.3%

問 2-2 第 1 問=27.4%、第 2 問=72.6%

問 2-3 第 1 問=34.2%(理解しやすいから，知識は多いほうが良い…)、第 2 問=65.8%(実際の画面だから、第 1 問の内容は学習済み…)

問 3　習得するのに 有効=93.2%、でない=6.8%、

確認するのに 有効=94.5%、でない=5.5%

図 3 に電子メールに関する 2018 年度宮崎大学情報セキュリティ対策講習のテスト結果、図 4 に疑似体験型 Web テスト電子メールのテスト結果、図 5 に疑似体験型 Web テスト Web ブラウザのテスト結果を表示する。

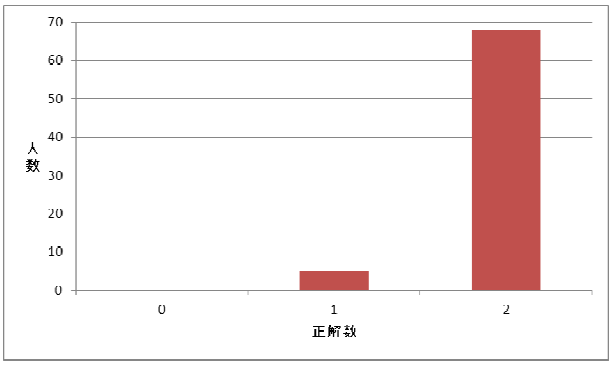

図 3　電子メールに関する 2018 年度宮崎大学情報セキュリティ対策講習のテスト結果

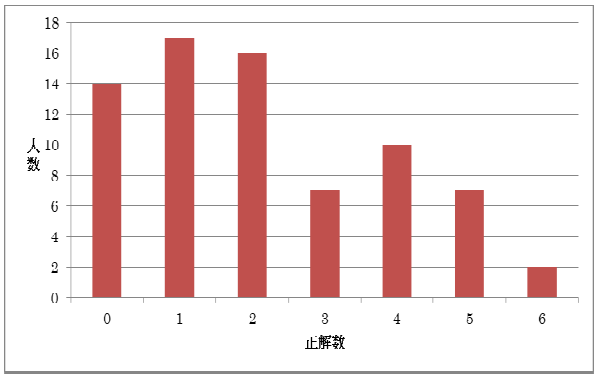

図 4　Web テスト電子メールテスト結果

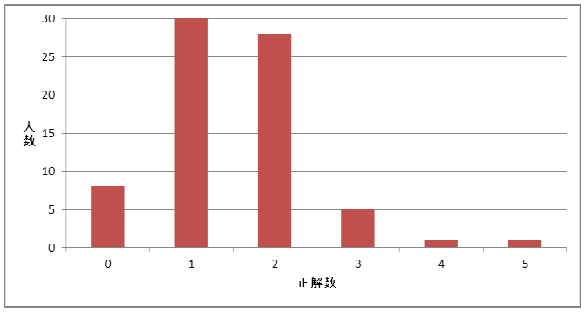

図 5　Web テスト Web ブラウザテスト結果

4 考察

アンケート問 1 では約半数が過去に解いた問題を覚えていないと答えているが、過去問題のテスト結果は正解率が非常に高く 2018 年度宮崎大学情報セキュリティ対策講習の問題を解くことについては十分に成果を上げているといえる。

一方アンケート問 2-3 実際のパソコン利用で役立つかどうかを問う質問において第 2 問を選んだ学生は第 1 問の約 2 倍であることと自由記述解答のうち第 2 問の方が役に立つと答えた理由として実際使用しているソフトウェアの画面であることを理由に挙げている事から疑似体験型 Web テストは従来型回答選択肢列挙タイプ e-learning 確認テストより実際のパソコン利用における情報セキュリティ対策の行動を再現しているものだと考えてよさそうである。

Web テストが実際の情報セキュリティ対策の行動を再現できること、電子メールに関する従来型回答選択肢列挙タイプ e-learning 確認テスト(第 1 問)の正解数と疑似体験型 Web テスト(第 2 問)の正解数の相関係数=-0.0078 で相関はないことから、従来型回答選択肢列挙タイプ e-learning 確認テストでは実際の情報セキュリティ対策にほとんど役立っていないと推測される。これは e-learning 確認テストの問題文を見ると判る。e-learning 確認テスト問題文は全ての状況を文章で回答者に提示しているのに対して Web テストは最初に情報セキュリティ対策上の問題が何処にあるか探し出すことを第 1 段階の問題としている。つまり回答能力が全く異なっている。

疑似体験型 Web テストは各情報セキュリティ対策に対する回答を求める従来型回答選択肢列挙タイプ e-learning 確認テストに答える前にユーザが普段利用しているソフトウェア画面イメージでユーザ自らが情報セキュリティ対策において注目すべき点を探る設問を設けたものだと考えている。その推測から正解領域をクリックした後の第 2 段階の設問の正解率(=正解数/回答した正解領域数)は従来型と同程度であると推測できる。しかし比較実験結果からは従来型回答選択肢列挙タイプ e-learning 確認テストの正解率=0.96 と Web テストで正解領域をクリックした場合の正解率=0.46 は明らかに異なっている。この結果の理由は(1)実証実験の対象が新入学部 1 年生であったため情報セキュリティ対策に対する知識が足りなかったか(2)疑似体験型 Web テストの設問が 2018 年度情報セキュリティ対策の講義内容を超えて出題されていたためではないかと考える。例えば電子メールに対するセキュリティ対策の一つ標的型メール攻撃への対策として「電子メールの差出人を確認することは"日頃メールのやり取りのない企業からのメール"」として IPA の電子メール利用時の危険対策のしおり[6]21 ページに載っているが、2018 年度速習版 INFOSS 情報倫理第 3 章インターネット上のコミュニケーション 3-1 電子メールによる被害

にはこの様な記述は載っていない。理由(1)の検証として別の学年を対象に実証実験を継続する予定である。今回の比較実験では ID、問題の正解数、不正解数、不正解領域数の回答数を収集し問題ごとの正解、不正解については収集していない。もし(2)の理由でテスト結果が振るわないのならば疑似体験型 Web テストの設問ごとにばらつきが出ると考える。次回以降の比較実験は出来れば問題ごとの結果を取得することを目指す。

最後に今回開発した疑似体験型 Web テストの利用方法について考える。疑似体験型 Web テストはユーザが利用するソフトウェアの表示画面を利用している。ユーザが良く利用するソフトウェアは電子メール、Web ブラウザ等数が少ないのでテストのバリエーションが非常に少なり何度も問題を解くと同じ問題が出てくる可能性が高くなる。また基本的に禁止事項に対する問題は作りにくい。例えば無断で著作物の複製を作ってはいけないという禁止項目に対する画面イメージをどの様に作ればよいか考えが浮かばない。以上のことから疑似体験型 Web テストは知識を深めるあるいは定着させるために複数回受ける問題というよりもっぱら学習度合い確認のためのテスト向けと考えられる。疑似体験型 Web テストは従来型の e-learning にとって代わるものではなく使い分けをする必要があると考える。

参考文献

[1] 日本データパシフィック株式会社、INFOSS 情報倫理 2018 年度版、https://www.datapacific.co.jp/u-assist/contents/mrl008.html.

[2] 情報処理推進機構、フィッシング(Phishing)対策、https://www.ipa.go.jp/security/personal/protect/phishing.html

[3] 情報処理推進機構、標的型攻撃メール<危険回避>対策のしおり、https://www.ipa.go.jp/security/antivirus/documents/10_apt.pdf

[4] 株式会社クオリティア、DEEPMail、https://www.qualitia.co.jp/product/dm/

[5] Mozilla、Firefox、https://www.mozilla.org/ja/firefox/

[6] 情報処理推進機構、電子メール利用時の危険対策のしおり、https://www.ipa.go.jp/security/antivirus/documents/07_mail.pdf