K-034

UIEを用いた一般ユーザ向けソーシャルエンジニアリング対策教材の評価

Evaluation of General Users Teaching Materials against Social Engineering Based on UIE

千葉 緑* 加藤 貴司* ベッド B. ビスタ* 高田 豊雄*
Midori Chiba Takashi Katoh Bhed Bahadur Bista Toyoo Takata

1 はじめに

ソーシャルエンジニアリングを含む情報セキュリティ教育は, 専門用語が多く文章が難しいなどの問題が指摘されている. このような問題を解決するため, GBS(Goal Based Scenario) 理論 [1] を適用した教材の開発が行われている. この GBS 理論を適用した教材を使用した学習では, ユーザはあらかじめ決められた役を演じながら学習する. しかし, その役がユーザにとって非現実的である場合には, 危機感を持ちにくいという問題がある. そこで我々はこの問題を改善するため, ユーザの身の回りを取りまくものや状況という UIE (情報活用環境:User's Information usage Environment) を考慮し, これを反映した教材を開発した [2]. 本稿では, 教材に反映した UIE の有効性の評価について述べる.

2 UIE (User's Information usage Environment)

2.1 GBS 理論

GBS 理論とは, 行動することによって学ぶシナリオ型教材を設計するためのインストラクショナルデザイン (Instructional Design) 理論である [1]. これは, 現実的な文脈の中で「失敗することにより学ぶ」経験を擬似的にあたえるための学習環境として物語を構築する理論である. GBS 理論を適用した教材でユーザは, 学習に必要な知識・技能を意味づけしたストーリーの中で学習を進める. このストーリーでは, ユーザに対して意味のある質問をシステムが出題する. この問題に対してユーザが回答を行うことによって, 自らで発見的学習をしていく.

GBS 理論を適用した情報セキュリティ教育教材においては, 達成感があり, 面白く, 重要な点も理解しやすかったなどの効果が得られている.

しかし, GBS 理論を適用した教材では, ユーザが「役割」として学習を進める必要がある. 例えば, ユーザが会社に勤めた経験のない場合, 会社に勤めている役を演じながら学習をしても, 現実的とは受け止めにくいため, 危機感を持ちにくい.

表 1: UIE の例

UIE の項目	ユーザ A	ユーザ B
通学している学校・通勤している会社の名前	岩手県立大学	C 会社
友達, 同僚とメールで連絡を取る際には, PC・携帯電話どちらをよく使うか	携帯電話	PC
現在住んでいる自宅に固定電話はあるか	ない	ある
電話の着信が多いのは, 携帯電話, 固定電話どちらか	携帯電話	固定電話

2.2 UIE

この問題点を解決するため我々は, GBS 理論を導入した教材に, ユーザの UIE(情報活用環境: User's Information usage Environment) という概念を新たに導入し, これをソーシャルエンジニアリング対策教材に反映させることを提案した [2].

UIE とは, ユーザの日常生活において, 身の回りを取り巻くものや状況のことである. ユーザはそれぞれ独自の環境を持っている. 例えば,「メールを送信する」際, 携帯電話を使用する頻度が高いユーザもいれば, PC を使用する頻度が高いユーザもいる. また,「買い物をする」際も, ユーザによって, 場所, 買う物などが異なる. このような, ユーザによって固有の UIE を利用し教材を変化させることで, ユーザにとって学習内容が想像しやすくなると考えられる.

2.3 UIE を適用したソーシャルエンジニアリング対策教材の例

1 日の生活を通じてどの場面で攻撃を受ける危険性があるかを学習するストーリーの場合, UIE を適用すると次のようになる.

例えば, ユーザ A, ユーザ B の UIE が表 1 のようになっていた場合, この情報を反映させることにより, それぞれ以下のようなストーリーで学習を行うことが出来る. 太字は, UIE を適用することで変化した部分である.

ユーザ A 岩手県立大学に通っているユーザ A は, 友達と課題をしている時, 先生から CD-R を処分して

*岩手県立大学大学院ソフトウェア情報学研究科, 〒 020-0193 岩手県岩手郡滝沢村滝沢字巣子 152-52, Iwate Prefectural University, 152-52, Sugo, Takizawa, Takizawa village, Iwate 020-0193.

くれと頼まれ, 友達と処分を試みる. その後帰宅したユーザ A は, 友達とメールで連絡を取っている時, 携帯電話に同窓会を開くため, 名簿に記載されている個人情報の確認をしているという内容の電話が来る.

ユーザ B 会社 C に勤めているユーザ B は, 会社で仕事をしている時, 先輩から CD-R を処分してくれと頼まれ, 処分を試みる. その後帰宅したユーザ B は, 同僚とメールで連絡を取っている時, 自宅の固定電話に同窓会を開くため, 名簿に記載されている個人情報の確認をしているという内容の電話が来る.

3 UIE を反映した教材の評価

我々は, GBS 理論を適用した教材の問題点を解決するために, GBS 理論を適用し UIE を反映したフィッシング対策教材を開発した. 本フィッシング対策教材では, ある会社を名乗りアンケートに答えて欲しいという内容の URL 付きメールが届き, URL をクリックするように誘導する. その URL をクリックしアンケートを入力すると, お礼を送付するために個人情報を入力するように言われる, というストーリーになっている.

3.1 フィッシング対策教材時の UIE

フィッシング対策教材では, ストーリーの内容を考慮し, UIE として以下の項目を設定した.

- 携帯電話と PC の使用頻度
- メールの契約会社
- 現在使用中の SNS(Social Network Service)
- 購読しているメールマガジン名
- 持っているポイントカード
- 在学中の学校名

この UIE について, ユーザごとに教材を使用する前に調査し, 教材に反映した.

3.2 評価内容

提案した UIE の有効性を評価するため, 本学の学生計 60 名を対象に以下の 3 つの教材を使用してもらった.

テキスト教材 「情報 C」[3] を使用した教材
GBS 教材 GBS 理論を導入した教材
提案教材 GBS 理論を導入し, UIE を反映させた教材

ここで, GBS 教材とは, GBS 理論に基づき作成した教材であり, ユーザがストーリーの中で学習する教材である. GBS 教材にユーザの UIE を反映した教材が提案教材である.

評価項目は以下の 2 点である.

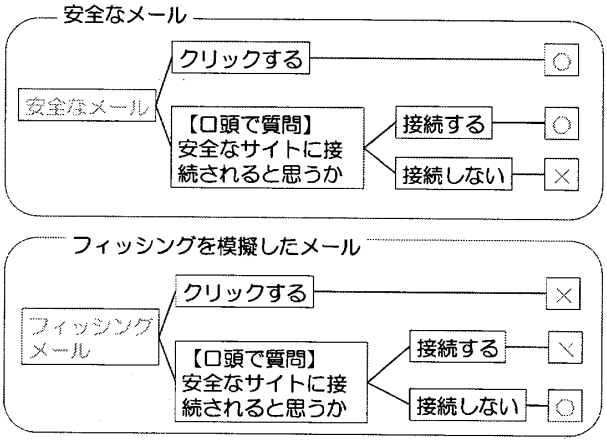

図 1: 態度・技能テストの判定方法

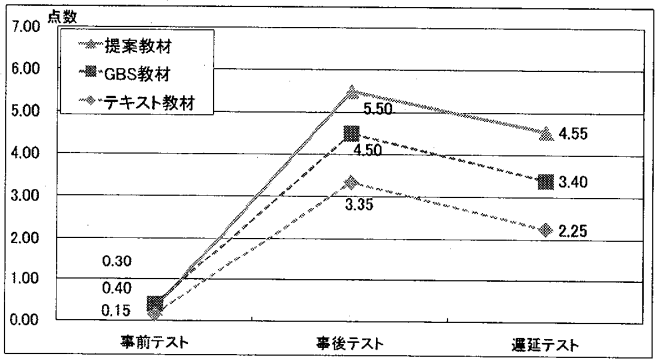

図 2: 評価項目 1 におけるテスト結果

評価項目 1 攻撃手法を理解できる.
評価項目 2 攻撃かどうかを判断し対処することができるようになる.

評価項目 1 については, 以下の 3 つのテストを行った.

1. **事前テスト** 学習の前に行うテスト
2. **事後テスト** 学習を行った直後に行うテスト
3. **遅延テスト** 学習を行った一週間後に行うテスト

評価項目 2 については, 遅延テストの後に態度・技能のテストとして行った. 態度・技能のテストでは, ユーザに URL 付きの 8 通のメールを送信し, そのときの行動から判断した. メールの内容は, 正規メール/フィッシングメール, PC/携帯電話, ユーザに関係のあるメール/関係のないメールの 3 項目の組み合わせ (8 通り) である. この 8 通のメールをユーザに送信し, その時のユーザの行動を判断した. ユーザの態度・技能の判定は, 図 1 のように行った.

これらの評価終了後に, 使用感を尋ねるためインタビューを行った.

3.3 評価結果

評価項目 1 UIE の有効性の評価実験結果を表 2, 図 2 に示す. 表 2, 図 2 中の事前テストと事後テストの

表 2: UIE の有効性の評価実験結果

		事前テスト (7 点満点)	事後テスト (7 点満点)	遅延テスト (7 点満点)	態度・技能テスト (8 点満点)
テキスト教材	平均	0.15 (2)	3.35 (48)	2.25 (32)	4.35 (54)
	標準偏差	0.49	1.81	1.94	0.75
GBS 教材	平均	0.40 (6)	4.50 (64)	3.40 (49)	5.05 (63)
	標準偏差	0.75	1.67	1.53	1.10
提案教材	平均	0.30 (4)	5.50 (79)	4.55 (65)	7.35 (92)
	標準偏差	0.92	1.28	1.60	1.14

※平均の欄の括弧内の数値は, 100 点満点換算したものである.

結果より, テキスト教材・GBS 教材・提案教材を使用することで, フィッシングについての知識がついたことが分かる. しかし, GBS 教材とテキスト教材では差が 1 点以上あり, 提案教材とテキスト教材の差も 2 点以上ある.

事後テストの結果より, ユーザはいずれかの教材を使用して学習を行うことで, 学習を行う前よりフィッシングについての知識をつけることは出来たと言える. その中でも, 提案教材を使用して学習を行った場合, 点数が高くなっている. このことより, ユーザが提案教材を使用した学習を行うことで, 他の教材よりも知識をつけることが出来たと言える.

これらの結果より, 提案教材を使用することで, 他の教材を使用した学習よりも攻撃手法を理解できている. すなわち, UIE を教材に反映し, これを用いて学習することは, フィッシング対策に対して有効であると言える.

一方, 遅延テストの平均点は, どの教材を使用しても事後テストの平均点から約 1 点下がっている. すなわち, 学習してから期間が空くと学習内容を忘れてしまうことが分かる. したがって, いずれの教材においても, 反復練習などが必要であると考えられる.

評価項目 2　態度・技能テストを行った結果を図 3, 4, 5 に示す.

テキスト教材 (図 3) 回答の内訳では, テキスト教材を使用したユーザの約 70%が 8 通全てのメールを正規メールと判断していた. 特に自分に関係のあるものに対しては全て安全であると判断してしまう傾向があり, これらのことから, フィッシングメールを正しく見分けることが出来ていないと言える.

これらの結果から, テキスト教材を使用した学習では, ユーザは正しい対策を身につけることは出来なかったと言える.

GBS 教材 (図 4) 回答の内訳では, GBS 教材を使用したユーザの約 45%が 8 通全てのメールを正規メールと判断した. また, GBS 教材を使用したユーザの約 90%がフィッシングメールの 4 通のうち, 自分と関係があるメールの一方または両方を正規メールと判断した. また, 正規メールをフィッシングメールと判断したユーザもいることから, GBS 教材では正規メールとフィッシングメールを正しく見分けることが出来ていないと言える.

これらの結果から, GBS 教材を使用した学習では, テキスト教材を使用した場合よりフィッシングメールを見分けられるようになっていると言える. しかし, 正規メールとフィッシングメールを完全に見分けることは出来ていない. そのため, GBS 理論のみを適用した GBS 教材では正しい対策を十分に身につけることは出来なかったと言える.

提案教材 (図 5) 図 5 より, ユーザのほとんどが正規メールとフィッシングメールを正しく見分けることが出来ていることが分かる. さらに, 回答の内訳では, 提案教材を使用したユーザの約 65%が全てのメールを正しく判断できていた. また, 提案教材を使用したユーザの約 80%がフィッシングメール 4 通を全て正しく見分けることができ, 約 85%がフィッシングメール 4 通のうち自分と関係がないメール 2 通全てを正しく見分けることが出来ていた. すなわち提案教材を使用したほとんどのユーザが, 正規メールとフィッシングメールを見分けることが出来ていると言える.

これらの結果から, GBS 理論を適用し UIE を反映した提案教材を使用した学習を行うことで, ユーザは正しい対策を身につけることが出来たと言える.

評価項目 2 の結果より, 提案教材を使用したユーザは, 正規メールとフィッシングメールを正しく見分けることが出来たと言える. これらの結果より, 提案教材は, テキスト教材や GBS 教材とは異なり, 正しい対策を身につけることが出来たと言える.

また, インタビューの結果は以下の通りであった.

テキスト教材 テキスト教材を使用したユーザからは, シンプルにまとまっている, つまらない, 興味が持てない, 眠くなるなどの意見が得られた.

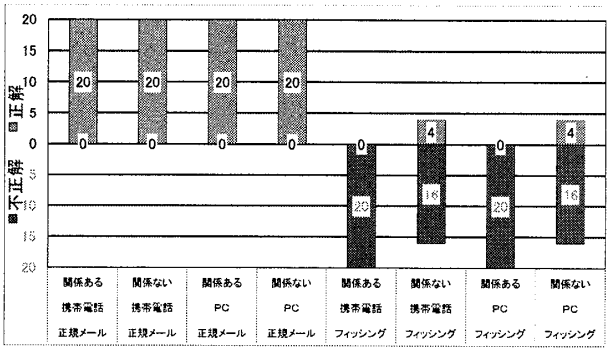

図 3: テキスト教材の態度・技能テスト結果

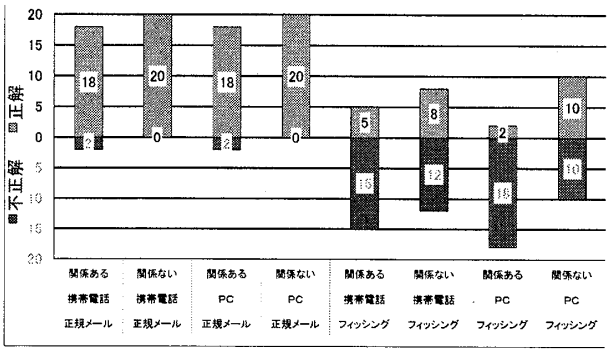

図 4: GBS 教材の態度・技能テスト結果

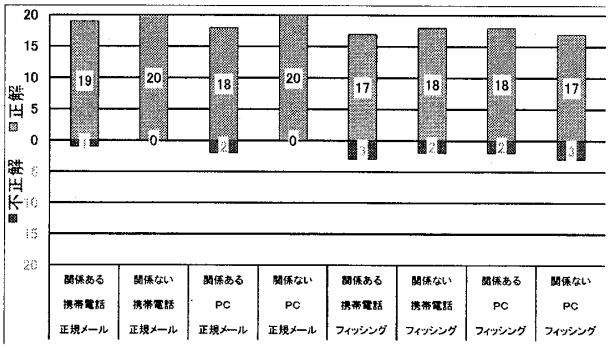

図 5: 提案教材の態度・技能テスト結果

GBS 教材 GBS 教材を使用したユーザからは, シミュレーションが楽しい, Web で体験しながら勉強が出来て楽しかった, 役になりきって出来たなどの意見が得られた.

提案教材 提案教材を使用したユーザからは, 自分の行動に対応した説明をしてくれるのでフィードバックしやすい, 日常に見立てて進行が楽しく, ただやるよりもリアリティがある, 事例をふまえて説明してくれる教材で楽しい, などの意見が得られた.

インタビューの結果より, UIE を反映した提案教材を使用し学習することで, より楽しく学習しながら知識を得ることが出来たということが言える.

4 おわりに

本稿では, 我々が開発した UIE を反映したソーシャルエンジニアリング対策教材の評価を行った. 評価結果より, テキスト教材や GBS 教材を使用した学習より, UIE を反映した提案教材を使用した学習の方が, ユーザは学習内容をイメージしやすく, かつ容易に理解し, 攻撃かどうかを見分けることが出来るようになったと言える. すなわち, GBS 理論を適用し本提案手法 UIE を導入した提案教材を使用することで, ユーザは正しい対策を身につけられるという効果が得られる.

今後は, フィッシング以外のソーシャルエンジニアリングの手法について, UIE の有効性を検証するために, UIE を適用した教材の開発, 評価を行う予定である.

謝辞

本稿において, GBS 理論を適用した教材の作成にあたり, ご指導頂いた岩手県立大学大学院の藤原康宏講師にこの場を借りて御礼申し上げます.

本研究は一部科研費 (基盤研究 (C)20500072) の助成を受けている.

参考文献

[1] Schank, R. C., Berman, T. R., Macpherson, K. A.: Learning by Doing. In Reigeluth, C. M. (ed), *Instructional-Design Theories and Models : A New Paradigm of Instructional Theory,* Volume II, pp. 161–181. Mahwah, NJ: Lawrence Erlbaum Associates. (1999).

[2] 千葉 緑, 加藤 貴司, 藤原康宏, Bhed Bahadur Bista, 高田豊雄: 情報活用環境を用いたソーシャルエンジニアリング対策教材の開発: 2009 年暗号と情報セキュリティシンポジウム (SCIS2009), 2D1-4 (2009).

[3] 坂村健 ほか 16 名: 三訂版 情報 C, 数研出版 (2007).