5W-04

動画コンテンツによる疑似的訓練を可能とする標的型攻撃教材の開発

八藤後　茉央† 　小倉　加奈代† 　Bhed Bahadur Bista† 　高田　豊雄†
岩手県立大学ソフトウェア情報学部†

1　はじめに

情報やシステムを守るためのセキュリティ技術は年々向上し，ネットワーク外部からシステム内部に侵入する攻撃の難度は高くなっている．それに伴い，標的型攻撃と呼ばれる情報の不正取得を目的として直接人間を狙う攻撃が台頭し始めている．攻撃者は攻撃対象から機密情報を窃取するために，攻撃と気づかれないような文章と一緒に不正なWebサイトへのURLや攻撃スクリプトを含んだファイルをメールやメッセージに添付して送信する．このような攻撃では人間の脆弱性を狙ったソーシャル・エンジニアリングと呼ばれる手法が利用されることが多く，技術的な方法だけでは対策が困難であり，信憑性のある文章などで標的が信じやすい手口を使う，被害者が攻撃自体に気づきにくいという特徴がある．これらの特徴を持つ攻撃への対策としては，セキュリティ教育のような人的対策を検討する必要がある[1].

本稿では，人間の脆弱性を狙った標的型攻撃への対策として訓練型の教育手法の提案し，その有効性を検証する．なお，訓練型の教育を行う理由は，様々なシチュエーションが想定される標的型攻撃の場合，学習者に具体的経験をさせることで攻撃への耐性を高める訓練型の教育手法がより効果的であるためである[2].

2　関連研究

2.1　訓練型セキュリティ教育事例

木村[3]は，セキュリティ対策が不完全な中小企業の従業員を対象にした訓練型のセキュリティ教育としてメール攻撃危険予知訓練システムを提案した．システムでは学習者の業務形態に合わせた訓練用の標的型攻撃メールを作成，送信する．このような訓練手法は，油断している学習者に突然模擬攻撃を行うことで標的型攻撃への対応として学習者が実際に行う行動を確認することができるが，以下のような運用上の問題がある．

(1)学習者の所属する組織におけるセキュリティポリシや環境に影響を受ける可能性がある．
(2)実在する団体や個人と似た名称を使用する場合，学習者が無関係な人へ問い合わせを行なう危険性がある．
(3)模擬攻撃メール作成のために，あらかじめ学習者やその所属する組織について調査を行う必要がある．

Development of Targeted Attack teaching Materials enabling pseudo training using Video Contents
†Iwate Prefectural University

2.2　ソーシャル・エンジニアリング教育事例

千葉[4]は，ソーシャル・エンジニアリングを利用したフィッシング攻撃に対する教材に，ユーザの身の回りの環境や状況を指す情報活用環境：User's Information usage Environment(以下，UIE)を取り入れることを提案した．既存教材である，ユーザに『役割』を持たせた攻撃シナリオを体験させるGoal Based Scenario理論[5]を適用した教材は『役割』の使い方によっては学習者が危機感を持ちにくくなる可能性があるという問題点がある．そこで教材に学習者や友人の名前，所属団体の名称などのUIE を反映して教材にリアリティを持たせることで危機感を持たせやすくし，実際に攻撃を受けた場合に学習者が教材による学習体験を想起しやすい教材を開発した．しかし，千葉の研究では主になりすましを利用したフィッシングメールに関する教材を取り扱っており，他の攻撃手法を用いた際の有用性は検討されていない．

3　提案手法

本研究では，Webサーバ上に公開した動画コンテンツを利用した人間を狙った標的型攻撃対策となる訓練・体験型のセキュリティ学習教材を提案し，その有効性を検証する．提案教材は一連の訓練がWeb上で完結する構成のため，2.1節の関連研究に見られるような運用上の問題が生じる恐れがない．また，視覚的に伝わりやすい動画というコンテンツにUIEを使用することにより，学習者が教材をリアリティのあるものとして使用することも期待できる．

3.1　提案システムの構成

提案教材では，あらかじめ訓練用 Web サーバに模擬攻撃動画を用意する．学習者は訓練用 Web サーバへ公開されている模擬攻撃動画へアクセスし，閲覧することで訓練を行う．

3.2　模擬攻撃動画

模擬攻撃動画は攻撃シナリオに沿ったインタラクティブな動画で，動画内の選択肢に応じて結果が変わる動画である．本研究では，メールとショートメッセージサービス(以下，SMS)による攻撃を想定した動画を使用する．2.1節や2.2節のような既存の標的型攻撃に対する訓練教材では，攻撃者からのコンタクト手法としてメールが選択されることが多かったが，現在はSMSを利用した標的型攻撃が行われる可能性もあるため，本稿ではメールとSMSを対象に訓練を行うこととする．

また，提案教材では標的型攻撃の手法を，危険なURLを利用するもの，情報漏洩を狙うもの，添付フ

ァイルを開かせるものの3つに分類する(図1)．提案教材を利用した訓練の際，学習者はそれぞれの手法の模擬攻撃動画を1つ以上閲覧し，標的型攻撃を体験する．

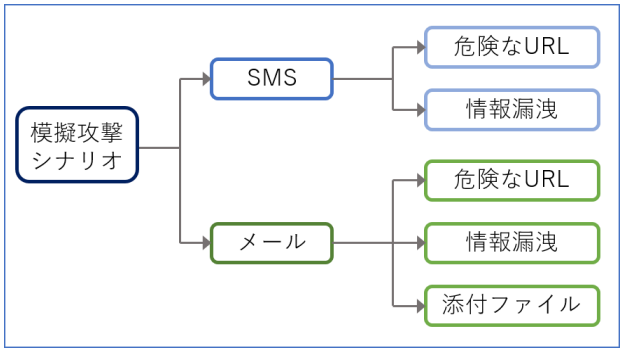

図 1:標的型攻撃の分類

図2は，模擬攻撃動画の一部である．学生の学習者に対して学校の医務機関を装った攻撃者から，感染症が流行する季節になったので添付ファイルの対策のしおりを確認してほしい，という実際に起こり得るメールを受信する動画である．この例では，添付ファイルにスクリプトが埋め込まれており，添付ファイルを開く選択肢を選択した場合は，動画の結末が埋め込まれていたスクリプトが起動しフォルダ内のファイルを勝手に攻撃者の元へ転送するという内容になる．選択肢によってはメールアドレスがフリーメールのものであることや過去に医務機関から届いたメールにはファイルが添付されたものがないことなどを確認することも可能であり，その場合はメールを削除することで攻撃を回避する結末になる可能性もある．

図 2:模擬攻撃動画の例

また，模擬攻撃動画には2.2節で述べた千葉の研究で有効性があるとされたUIEを取り入れ，学習者がより危機感を感じられるようにする．例として図2のメールの場合では，学習者があらかじめ入力した学校名によって本文内の学校の名称や医務機関の名称が変更される．

4 評価

提案教材の有効性を評価するため，筆者の所属する学部学生(以下，協力者)に提案教材を実際に使用してもらい評価する．4.1節より詳細を説明する．

4.1 形成的評価

有効性評価に使用する教材を開発し，形成的評価を行った．教材の使用方法を説明し，教材を使用させ，その感想を尋ねた．「堅苦しい教材感がなく興味が沸いた」など，学習者のモチベーション向上を示す感想を得ることができたが，「動画内に音による影響が少ないのではないか」のような意見もあり，文字の見やすさなどと共に修正した．

4.2 動画教材の有効性評価

協力者を3グループに分け，模擬攻撃動画を利用した教材，文字のみの教材，文字に加え画像を使用した教材を使用してもらう．協力者には教材を使用する前に前提・事前テスト，教材を使用した後に事後テストを行い，点数を評価する．また，教材の使用感についても協力者へのインタビューを行い，各教材での比較を行う．

4.3 提案手法の有効性評価

協力者に図1で分類した3種類の模擬攻撃動画を用いた教材を使用させる．協力者は事前に事前テストに回答し，教材使用後に行う事後テスト，教材を使用した1，2週間後に行う遅延テストと点数を比較することで学習効果を評価する．

5 おわりに

本稿では，学習者のセキュリティ意識の向上や人間を狙った標的型攻撃への耐性を高めることを目的とし，動画コンテンツを利用した訓練形式の標的型攻撃対策手法を提案した．特に，SMSを利用した攻撃は今後さらに増加すると考えられ，教育を行う必要がある．提案教材は既存の教材よりも学習者が興味を持って取り組める教材になると考えられる．

謝辞　本研究はJSPS科研費16K01025の助成を受けたものである．

参考文献

[1] 内田勝也：標的型メール攻撃に対するセキュリティ心理学・セキュリティマネジメントからの考察，経営情報学会全国研究発表大会要旨集，pp.65-68 (online)，DOI:10.11497/jasmin.2015f.0_65 (2015).
[2] 山口健太郎，小宮山功一朗，内田勝也：ユーザへの予防接種というアプローチによる標的型攻撃対策-2，情報処理学会第71回全国大会講演論文集（セキュリティ），pp.349-350 (2009).
[3] 木村壮太：メール攻撃危険予知訓練システムの開発，情報処理学会研究報告CSEC，2013-CSEC-63(4)，pp.1-6，(2013).
[4] 千葉緑：ソーシャルエンジニアリングの学習を支援するための教材開発に関する研究，岩手県立大学2010年度博士前期課程(ソフトウェア情報学)論文，(2010)．
[5] 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, Vol. II, pp.161-181. Mahwah, NJ: Lawrence Erlbaum Associates.(1999).