4F-04

体験型によるセキュリティ研修ツールの開発と評価

大久保　隆夫†　　青山　祐輔‡　　小村　誠一☆

情報セキュリティ大学院大学†　　株式会社企‡　　NTT アドバンステクノロジ株式会社

1. はじめに

筆者らは，重要インフラ分野の運用従事者を対象とした，サイバー攻撃等を擬似的に体験可能な教材を開発した．本稿はその教材の提案およびその評価について述べる．

2020 年の東京オリンピック，パラリンピックを控え，大会期間中やその前後におけるサイバー攻撃の危険がさけばれている．特に，電力や交通，通信，放送などの重要インフラは，一度攻撃を受けると大会の運営だけでなく社会にも交通麻痺や電力供給の停止など，社会にも深刻なダメージを与えかねない．したがって筆者らは，重要インフラの運用担当者を教育対象として教材の開発を行った．

セキュリティインシデントの適切な対応のためには，故障やヒューマンエラーなど他に発生している事象に加え、セキュリティインシデント発生時の状況がどのようなものか認識する能力が必要とされる．セキュリティインシデント発生時の切り分けをより適切に行なう能力の向上を図るため、インシデントの 1 次対応を行う運用従事者を対象とし，サイバー攻撃の基礎を体験的に学ぶ教材の開発を目標とした．

2. 従来技術と課題

サイバー攻撃を体験的に学ばせる手法としては，(1)スライドや動画を用いる手法［1］(2)実環境を用いる手法［3］(3)仮想環境を用いる手法［2]がある．

(1)のスライドや動画は，攻撃を受ける様子を時系列で利用者に体験させることはできるが，利用者のインタラクションがないため，利用者がどんな操作をしたらまずいことが起きてしまうのかという，当事者意識を持たせることがむずかしい．(2)の実環境を用いる手法は，攻撃を受ける実環境を用意し，攻撃により被害を受ける様子を実際に体験してもらうものである．この方法であれば，利用者の操作により，攻撃を受けて被害にあう様子を実際のインシデントと同様に体感することは可能である．ただし，ランサムウェアなどの場合，感染によって実環境は破壊されてしまうため，受講後に復旧などの作業が必要になる．(3)の仮想環境を用いる手法は，実環境ではなく仮想環境で体験するため，(2)の実環境とほぼ同等の体験が可能である．それに加え，(2)のように実環境を壊すことなく，マルウェアに感染した仮想環境は状態を戻すことで，再度の利用が可能になる．しかし，仮想環境はそれを実行するために一定のメモリ，CPU 性能と実行環境のソフトウェアが必要になる．このため，特に大規模の受講者を要する場合には計算機環境の用意が障害になり得る．また，(2)や(3)の手法では利用者の行動に自由度がありすぎるため，意図した操作をするためには適切な誘導や制約が必要になる．

3. javascript を用いた体験教材

筆者らは，既存手法の課題を解決するため，javascript を用いて攻撃の体験を提供する教材を開発した．教材の画面の例を図 1 に示す．

画面は Windows7 の画面をキャプチャして表示しているが，javascript を用い，マウスで対象領域をクリックやダブルクリックすることで，次の画面への遷移を実行する．この実装を利用し，利用者が不適切な操作を行うと，攻撃により被害を受ける様子をマウス操作のキャプチャと画面の遷移により表現している．図 1 はランサムウェア攻撃を説明する教材の画面である．ランサムウェアはメールの添付ファイルを開くことにより感染するので，メールの添付ファイルのアイコンおよびそれをクリックすることにより，感染が起きた場合の画面を用意することにより，添付ファイルの開封によりランサムウェアに感染する様子を利用者が体験できる．また，利用者の不適切な操作を誘導するため，次に操作すべき場所と操作内容を画面に吹き出し

Development and evaluation of a hands-on security training tool

†Takao Okubo, Institute of Information Security
‡Yuusuke Aoyama, Kuwadate inc.
☆Seiichi Komura, NTT Advanced Technology Corporation

図 1: 体験型教材の画面例

で表示する．これにより，利用者は攻撃により被害に合うシナリオを効率的に再現できる．

この教材に，通信事業者に聴き取りを行い，次の 6 つの攻撃シナリオを実装した．(1)ランサムウェア(2)フィッシング(3)バックドア(4)SQL インジェクション(5)SD カードからのマルウェア感染(6)Web カメラの脆弱性

4. 教材の評価

開発した教材の有効性について，セキュリティに関する技術経験の少ない学部生 9 名と，社会人を中心とする大学院生 10 名に受講させ，受講前と受講後で当該攻撃に関する知識状況を 5 段階評価してもらったところ，各攻撃シナリオの知識の向上率の平均が学部生，院生共に 25%であった．また，学部生の平均知識レベルが 3.2 だったのが，受講後は平均 4.0 になり，院生の受講前の知識平均 4.0 と一致した．このことから，セキュリティ知識に乏しい運用技術者に実装した教材を体験させることで，セキュリティ有識者に近いレベルまで引き上げることが期待できることがわかった．

5. おわりに

筆者らは，重要インフラ分野の運用従事者を対象とした，サイバー攻撃等を擬似的に体験可能な教材を開発した．教材はブラウザ上で動作するため，仮想環境や実環境を用意することなく，また実環境に影響を与えることなく利用者に攻撃を引き起こす不適切な操作やその影響を学ばせることが可能となる．また，開発した教材を学生に受講させ，知識の向上が見られることを確認した．

現在は，作成した教材を複数のインフラ事業者に試行してもらっている．今後，その評価分析と攻撃シナリオの拡充を行う予定である．

謝辞

本研究は内閣府が進める戦略的イノベーション創造プログラム(SIP)「重要インフラ等におけるサイバーセキュリティ確保」(管理法人 NEDO)の委託費により実施されました．

参考文献

[1] 神奈川県生活消費課，“「インターネットの危ない世界」を体験しよう！PART1,” 19 12 2019. [オンライン]. Available: https://www.pref.kanagawa.jp/docs/r7b/cnt/f535323/p415459.html. [アクセス日: 25 12 2019].

[2] IPUSIRON, ハッキング・ラボのつくりかた 仮想環境におけるハッカー体験学習，翔泳社，2018.

[3] 情報処理推進機構，“脆弱性体験学習ツール AppGoat,” 22 12 2019. [オンライン]. Available: https://www.ipa.go.jp/security/vuln/appgoat/. [アクセス日: 25 12 2019].