1ZA-04

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-

清時耀† 福田洋治‡ 井口信和‡

近畿大学大学院総合理工学研究科† 近畿大学理工学部情報学科‡

1. はじめに

近年，組織の構成員のセキュリティ意識を高めセキュリティ行動を促進するため，メールの受信や Web のアクセスから始まる誘導型攻撃の体験や演習ができるシステムが登場している[1)]．

著者らは，組織内で起こるセキュリティインシデントの再発防止において，実施されるセキュリティ訓練の円滑な実行の支援をするため，起こった事を分かりやすく伝える，組織内で起こった Web を介した攻撃を学習，体験できるセキュリティ訓練システム(以下，本システム)の開発を進めている[2)]．

本稿では，訓練を充実させるために 3 つのシナリオを追加した事と学習した内容が身についたか否かを確認する確認テスト部を試作した事について報告する．また，本システムが訓練の実行の支援が行えているのを確認する事を目的に，動作実験と確認テストによる本システムの評価を行った事も報告する．

2. セキュリティ訓練システム

セキュリティ訓練の円滑な実行の支援をする目的で，Web を介した攻撃を学習，体験できる訓練システムを開発する．このシステムの要件を以下に示す．

要件 1 … 組織で起こった Web を介した誘導型攻撃を含むインシデントを再現できること．

要件 2 … 個人に状況を判断，端末を操作させてその結果として何が起こるか体験できること．

要件 3 … 個人の端末操作の結果，起こった個々の事象について説明できること．

要件 1～3 を満たすシステムの構成を図 1 に示す．シナリオ作成者は，仮想環境構築ツールを用いて，攻撃対象ホストの OS 等を設定し，シナリオ作成部で訓練シナリオを作成する．訓練者

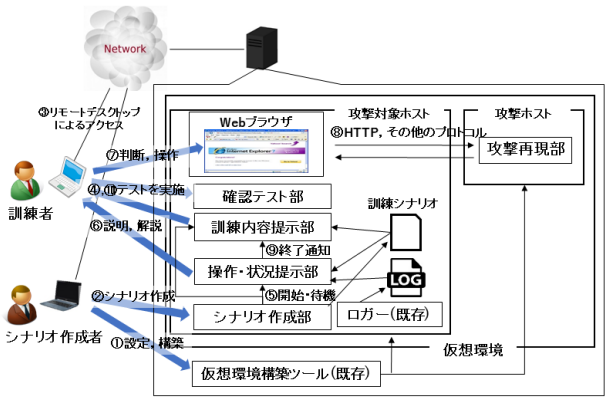

図 1 Web を介した誘導型攻撃の訓練システムの構成

は，攻撃対象ホストへリモートデスクトップ接続を行い，訓練を実施する．攻撃再現部は，ペネトレーションテストに用いられる Metasploit Framework のエクスプロイトを使用し，Web を介した誘導型攻撃を含むインシデントを再現する．再現の際には，サーバ構築等の再現環境の用意に，シェルスクリプト等を使用し，操作・状況提示部などが訓練シナリオを読み込んだ際に，シェルスクリプトが実行され，再現環境を用意する．攻撃再現部を稼働させた攻撃ホストと，攻撃対象ホストを配置して，訓練者にリモートデスクトップで攻撃対象ホストを操作させることにより，要件 1 と要件 2 に対応すると考えられる．シナリオ作成部は，インシデントの原因，事象の関係性と，訓練内容のメッセージなどから成る訓練シナリオの作成を支援する．訓練内容提示部は，訓練シナリオに基づいて，訓練者の立場・状況・仕事といった訓練内容のメッセージを提示する．操作・状況提示部は，訓練者の操作に応じて攻撃対象ホストのアプリケーション等の挙動を，ロガーの出力をモニタしながら訓練シナリオに基づいて未成立の事象の有無を判断し，各ノードのメッセージを提示する．これにより要件 3 に対応すると考えられる．

これらに加え，確認テスト部を試作し，本システムに追加した．確認テスト部は，Web ブラウザから確認テストのページを要求するリクエ

Development of Security Training System Enabling to Learn Mechanism and Experience of Incident - A Function Performing Evaluation and Comprehension Test of Training in Induction Attacks via Web –

†Akira KIYOTOKI, Graduate School of Science and Engineering, Kindai University

‡Youji FUKUTA, Nobukazu IGUCHI, Department of Informatics School of Science and Engineering, Kindai University

ストを受け取れば，確認テストの Web ページを生成し，確認テストのページをレスポンスとして返す．訓練者が Web ページの提出ボタンを押下すれば，解答結果を Web サーバに送信する．解答結果を受信すれば，採点を行い，正答数をレスポンスとして返す．これにより，訓練システム使用前後で，確認テストを実施できる．

また，元々あった標的型メール攻撃のシナリオに加え，ランサムウェアと偽警告，Skype 経由の情報漏洩を訓練システムにシナリオとして追加した．紙面の都合上，ランサムウェアのシナリオについて述べる．ランサムウェアは，ファイルが暗号化されるまたは，端末がロックされる等の PC の利用制限がかけられ，その制限解除と引き換えに金銭を要求するような挙動をする不正プログラム[3]である．本システムのランサムウェアのシナリオは，用意した Web サイトの悪意のある広告をクリックされれば，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表示される．このシナリオで，安易に広告をクリックしない事などが学習できる．

3. 動作実験と確認テストの実施

本実験では，本システムが訓練の実行の支援が行えているのを確認する事を目的に，本システムで実施した訓練の有効性を確認する．それに加え，シナリオを再生した際に，訓練システムが正しく動作する事も確認する．これらを確認するために，本システムで訓練を実施する前後に確認テストを実施し，正答数を計った．そして，前後の正答数の平均と標準偏差を求めた．確認テストの制限時間 24 分で，著者らが所属している研究室および，本学の他の研究室のメンバー12 名を対象に確認テストを行った．また，IT パスポートの問題を参考に作成した問題，合計 10 問を確認テストで出題した．確認テストは，被験者に確認テスト用紙を配布し，被験者にテストの内容を説明した．説明後，ストップウォッチで 24 分を計測した．24 分が経過後もしくは，解答を終えたものから，確認テスト用紙を回収した．そして，標的型メール攻撃などのシナリオを訓練システムで再生し，訓練を実施した．訓練の実施後，上記の手順で同じテストを実施し，最後テスト用紙を回収した．この流れを標的型メール攻撃，ランサムウェア，偽警告，Skype 経由の情報漏洩の 4 回実施した．そして Excel にデータを入力し，前後のテストの平均正答数と標準偏差を計算した．その結果，表 1 のようになった．計算した値は，小数点第 2 位で四捨五入を行った． 本実験から，本システムを用いて訓練を実施する前と後で，平均正答数が約 2~3 問増える事，標準偏差が 1~2 問である事がわかった．本システムを用いて訓練を実施する事で，知識を増やす事ができる．この事から本システムが知識を増やす上で，有効である事が分かった．また，訓練の実施した際に，追加したシナリオを含む 4 つのシナリオが意図したとおりに動作する事も確認した．今回，訓練実施後に正解している問題の多くは，操作・状況提示部で説明された内容が多かった．よって平均正答数の増加は，操作・状況提示部の説明が大きく影響していると考察する．この事から，操作・状況提示部で説明する内容を増やす事により，正答数を伸ばす事ができるのではないかと考える．

表 1　確認テストの結果

	平均(前)	平均(後)	標準偏差(前)	標準偏差(後)
標的型メール攻撃	6.83	8.83	1.28	1.07
ランサムウェア	6	8.25	1.63	1.3
偽警告	6.73	9	1.42	1.08
Skype経由の情報漏洩	6	7.58	2.22	1.93

4. まとめ

著者らは，組織内で起こるセキュリティインシデントの再発防止において，実施されるセキュリティ訓練の円滑な実行の支援をする目的で，起こった事を分かりやすく伝える，組織内で起こった Web を介した攻撃を学習，体験できるセキュリティ訓練システムの開発を進めている[2]．

実験から，本システムが知識を増やす上で有効であり，追加したシナリオを含む 4 つのシナリオが確かに動作する事も確認した．今後の課題として，訓練をより充実させるために，操作・状況提示部で説明する内容を増やす事が挙げられる．

参考文献

1) 八代哲，宮田大地ら: 標的型攻撃の体験ができる自習型演習システムの提案と実装，情報処理学会第 79 回全国大会，4W-04，pp.587-588（2017)

2) 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，電子情報通信学会関西支部学生会，vol.23，pp.14(2018).

3) トレンドマイクロ:ランサムウェア，トレンドマイクロ(オンライン)，入手先<https://www.trendmicro.com/ja_jp/security-intelligence/research-reports/threat-solution/ransomware.html>(参照 2019-01-09)